P. BACHMANN

DIE ARITHMETIK DER QUADRATISCHEN FORMEN



P. P.

Meinen umfangreichen Verlag auf dem Gebiete der **Mathematischen, der Technischen und Naturwissenschaften** nach allen Richtungen hin weiter auszubauen, ist mein stets durch das Vertrauen und Wohlwollen zahlreicher hervorragender Vertreter obiger Gebiete von Erfolg begleitetes Bemühen, wie mein Verlagskatalog zeigt, und ich hoffe, dafs bei gleicher Unterstützung seitens der Gelehrten des In- und Auslandes auch meine weiteren Unternehmungen Lehrenden und Lernenden in Wissenschaft und Schule jederzeit förderlich sein werden. **Verlagsanerbieten** gediegener Arbeiten auf einschlägigem Gebiete werden mir deshalb, wenn auch schon gleiche oder ähnliche Werke über denselben Gegenstand in meinem Verlage erschienen sind, stets sehr willkommen sein.

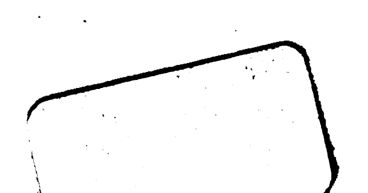
Unter meinen zahlreichen Unternehmungen mache ich ganz besonders auf die von den Akademien der Wissenschaften zu München und Wien und der Gesellschaft der Wissenschaften zu Göttingen herausgegebene **Encyklopädie der Mathematischen Wissenschaften** aufmerksam, die in 7 Bänden die **Arithmetik** und **Algebra**, die **Analysis**, die **Geometrie**, die **Mechanik**, die **Physik**, die **Geodäsie** und **Geophysik** und die **Astronomie** behandelt und in einem Schlufsband **historische, philosophische** und **didaktische Fragen** besprechen, sowie ein **Generalregister** zu obigen Bänden bringen wird.

Weitester Verbreitung erfreuen sich die mathematischen und naturwissenschaftlichen Zeitschriften meines Verlags, als da sind: Die **Mathematischen Annalen**, die **Bibliotheca Mathematica**, das **Archiv der Mathematik und Physik**, die **Jahresberichte der Deutschen Mathematiker-Vereinigung**, die **Zeitschrift für Mathematik und Physik** und die **Zeitschrift für mathematischen und naturwissenschaftlichen Unterricht.**

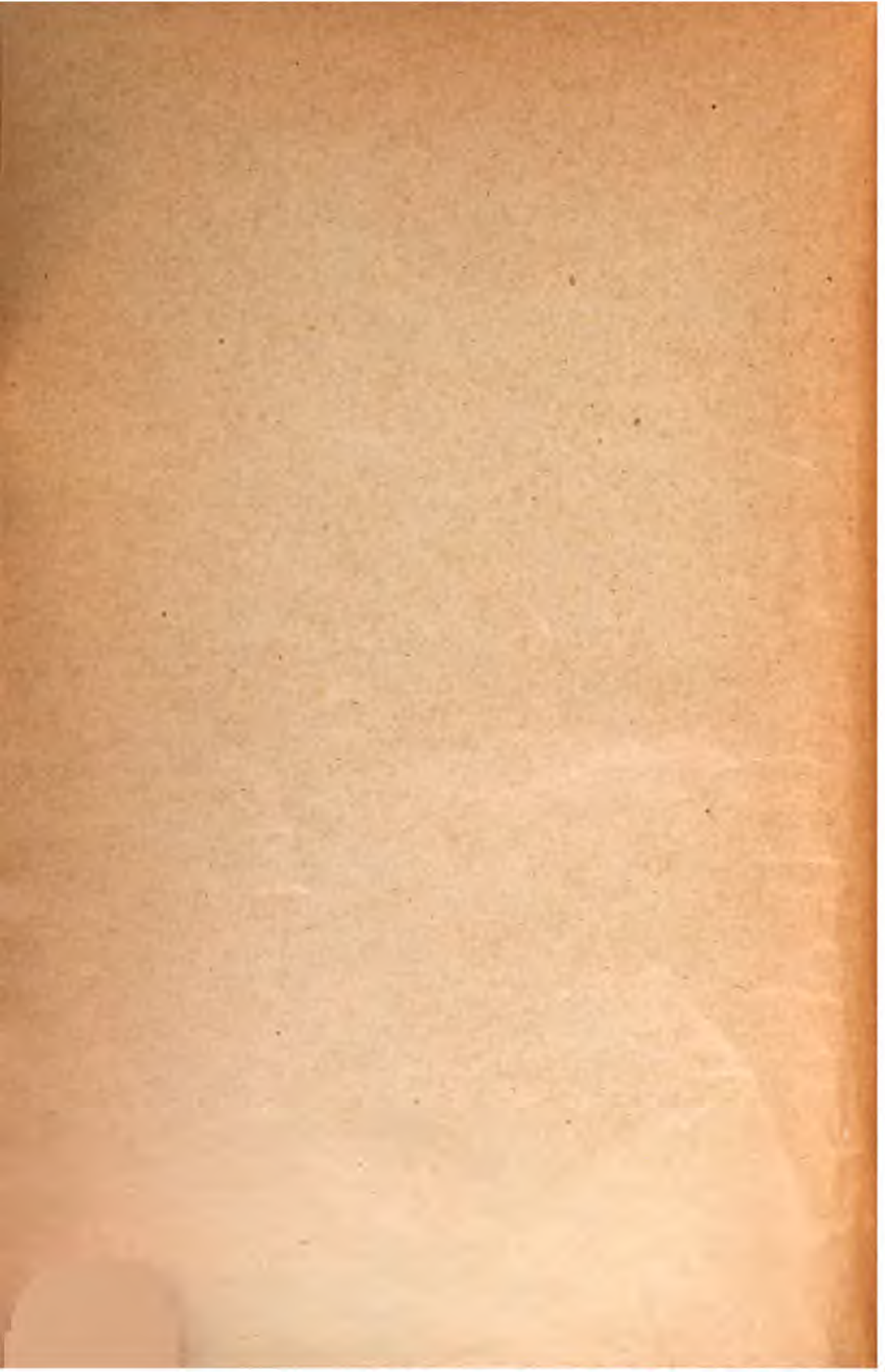
Seit 1868 veröffentliche ich in kurzen Zwischenräumen: **„Mitteilungen der Verlagsbuchhandlung B. G. Teubner“.** Diese „Mitteilungen“, welche unentgeltlich in 20 000 Exemplaren sowohl im In- als auch im Auslande von mir verbreitet werden, sollen das Publikum, welches meinem Verlage Aufmerksamkeit schenkt, von den erschienenen, unter der Presse befindlichen und von den vorbereiteten Unternehmungen des Teubnerschen Verlags in Kenntnis setzen und sind ebenso wie das bis auf die Jüngstzeit fortgeführte jährlich zwei- bis dreimal neu gedruckte **Verzeichnis des Verlags von B. G. Teubner auf dem Gebiete der Mathematik, der technischen und Naturwissenschaften nebst Grenzgebieten,** 95. Ausgabe [XXXVIII u. 140 S. gr. 8], in allen Buchhandlungen unentgeltlich zu haben, werden auf Wunsch aber auch unter Kreuzband von mir unmittelbar an die Besteller übersandt.

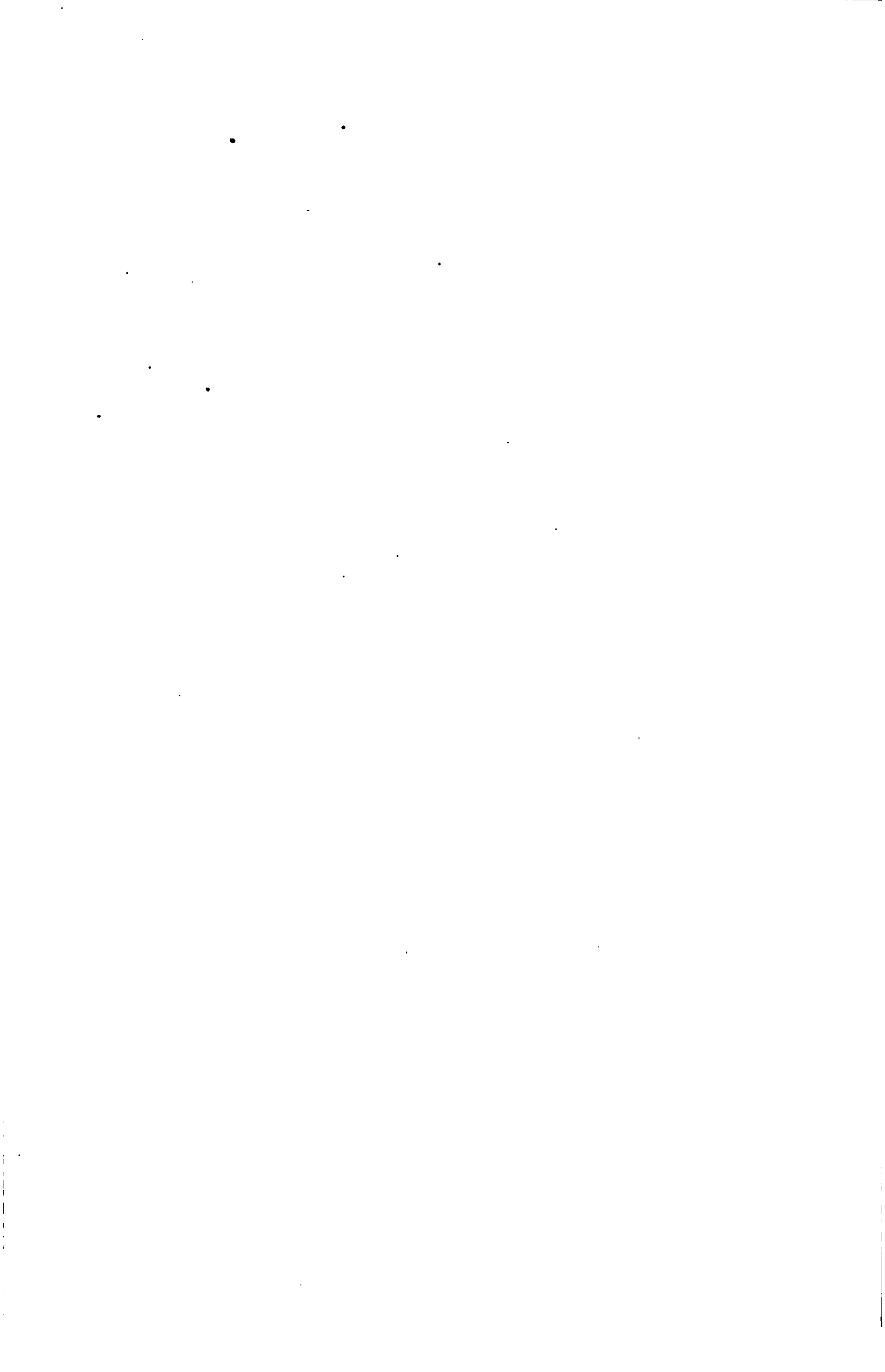
Leipzig, Poststrafse 3.

B. G. Teubner.









ZAHLENTHEORIE.

VERSUCH

EINER

GESAMMTDARSTELLUNG DIESER WISSENSCHAFT

IN IHREN HAUPTTHEILEN

VON

PAUL BACHMANN.

VIERTER THEIL.

DIE ARITHMETIK DER QUADRATISCHEN FORMEN.



LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1898.

DIE ARITHMETIK

DER

QUADRATISCHEN FORMEN.

DARGESTELLT

VON

PAUL BACHMANN.

ERSTE ABTHEILUNG.

LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1898.

Vorrede.

Den Elementen der Zahlentheorie und der Analytischen Zahlentheorie lasse ich mit diesem Werke den *vierten* Theil meines Gesammtunternehmens folgen, indem ich die früher von mir veröffentlichte Lehre von der Kreistheilung und ihren Beziehungen zur Zahlentheorie, deren Neubearbeitung ich mir vorbehalte, als *dritten* Theil desselben zähle. Das neue Werk giebt die *Arithmetik der quadratischen Formen mit einer beliebigen Anzahl von Unbestimmten.* Nachdem schon *Gauss* für die Theorie der *ternären* Formen die hauptsächlichsten Probleme gestellt und theilweise gelöst hatte, führten später namentlich *Eisenstein*, in neuerer Zeit St. *Smith* diese Lehre grösserer Vollendung entgegen; zugleich aber leitete die Ausdehnung der Probleme und Methoden des besonderen Falls zur Entwickelung einer Arithmetik der quadratischen Formen überhaupt, welche vornehmlich durch die Arbeiten von *Smith* und *Minkowski* bereits eine hinreichende Ausbildung erfahren hat, um eine einigermassen abgerundete systematische Darstellung zu gestatten. Das neue Werk soll eine solche versuchen; es zerfällt in *drei grössere Abschnitte.*

Der *erste* behandelt ausschliesslich die *ternären* Formen. Denn, getreu dem bisher eingehaltenen Verfahren, soll auch hier die Darstellung, soweit dies, ohne die Klarlegung des inneren Zusammenhanges der Lehre zu beeinträchtigen, geschehen kann, ihrer geschichtlichen Entwickelung Rechnung tragen. Zudem wird durch die vorgängige Darstellung der Lehre von den ternären Formen das Verständniss der viel schwierigeren allgemeinen Theorie wesentlich erleichtert werden, auch konnte nur in dieser Weise die Darstellung der

mannigfaltigen auf jene besonderen Formen bezüglichen Einzeluntersuchungen wünschenswerthe Abrundung erhalten. Nach einem einleitenden Capitel, welches die algebraischen Grundlagen der Theorie, insbesondere die algebraische Transformation der Formen in sich selbst giebt, folgt die Eintheilung der Formen in Classen, Ordnungen und Geschlechter nach Eisenstein und Smith; das nächste Capitel bringt die Gauss'sche Theorie der Darstellung, das folgende die Untersuchung aller ganzzahligen Transformationen einer Form in sich selbst, auf welche jene zurückführt. Nach einer kurzen Erörterung über die Geschlechter binärer Formen, welche auch den zweiten Gauss'schen Beweis des Reciprocitätsgesetzes enthält, wird das Vorhandensein der Geschlechter binärer sowohl wie ternärer Formen bewiesen und nach Einführung des Eisenstein-schen Begriffs vom Maasse der Formen zunächst die Anzahl der Darstellungen einer Zahl als Summe dreier Quadrate behandelt, woran sich Sätze über die Darstellbarkeit der Zahlen durch eine Summe von vier Quadraten und von Polygonalzahlen anschliessen. Ein weiteres Capitel bestimmt zuerst nach Eisenstein'scher Methode, sodann nach Smith das Maass eines Geschlechts sowie einer Ordnung positiver Formen, wobei, wie überhaupt, der Einfachheit halber die Determinante ungerade vorausgesetzt wird. Dann folgt eine zusammenhängende Darstellung der Arbeiten von Gauss, Dedekind, Cantor u. A. über die Gleichung $ax^2 + a'x'^2 + a''x''^2 = 0$, und zuletzt ein Auszug aus A. Meyer's Arbeiten über die Classenanzahl eines indefiniten Geschlechts u. dgl.

Der zweite Abschnitt ist den allgemeinen quadratischen Formen gewidmet. Soweit es zulässig ist, ohne Wesentliches zu beeinträchtigen, beschränke ich mich wieder auf Formen mit ungerader Determinante. Auch hier wird mit Zusammenstellung einiger algebraischen Hilfssätze und Betrachtungen begonnen. Nachdem dann die Zusammensetzung von „Zahlensystemen“ erörtert, gebe ich im folgenden Capitel auf Kronecker'scher Grundlage eine Lehre von den Elementartheilern solcher Systeme. Als Anwendung derselben erscheint in zwei weiteren Capiteln die Arithmetik der Linearformen, die Lehre von den linearen Gleichungen und Congruenzen.

Das hierauf folgende Capitel bringt als eine weitere Anwendung derselben Lehre nach Hermite, Rosanes und Frobenius die algebraische Transformation der Formen in sich selbst. Nunmehr folgt die eigentliche Arithmetik der quadratischen Formen, zunächst die Eintheilung der Formen in Classen, Ordnungen und Geschlechter, die genaue Bestimmung der Geschlechtscharaktere nach dem Vorgange von Smith und Minkowski. Das nächste Capitel enthält eine Untersuchung über quadratische Congruenzen, um die Grundlage zu liefern für die neue Definition des Geschlechts nach Poincaré und Minkowski, welche das folgende Capitel einführt. Im Zusammenhange damit steht die auch für das Folgende wichtige Bestimmung der Anzahl der „Reste", welche ein gegebenes Geschlecht in Bezug auf einen gegebenen Modulus haben kann. Nun giebt das nächste Capitel die Theorie der Darstellung einer Zahl oder einer Form mit $n-1$ durch eine solche mit n Unbestimmten. Nach Feststellung des Zusammenhangs zwischen den Geschlechtern beider Formen ergiebt sich der Nachweis für das Vorhandensein der zulässigen Geschlechter. Von hier ab werden nur noch positive Formen, insbesondere ihr Maass betrachtet, zunächst die Anzahl der Darstellungen einer Zahl als Summe von vier oder fünf Quadraten, sodann der schöne Minkowski'sche Ausdruck für das Maass eines Geschlechts von Formen, der aus den wesentlichen Faktoren der Maasszahl gebildet ist. Und hieran schliessen sich Betrachtungen über die Anzahl von Darstellungen einer Zahl als Summe von sechs oder mehr Quadraten und Aehnliches an.

Der dritte Abschnitt handelt von der Reduktion der Formen. Im Vorhergehenden bedurfte man nur des Princips der Reduktion, wesentlich zur Feststellung, dass die Anzahl der Classen für eine gegebene Determinante eine endliche ist. Die eigentliche Reduktion der quadratischen Formen, die präcise Fassung der reducirten Form und ihre wichtigen Folgerungen bilden ein eigenthümliches Gebiet der Zahlentheorie, welches theils durch die Rolle, die das Stetige darin spielt, theils durch die besonders wichtigen nicht-zahlentheoretischen Resultate, die aus ihm erwachsen: Grenzen für gewisse Minima, Annäherungsprocesse, wie die Kettenbruchalgorithmen, die der

arithmetischen Charakteristik der Irrationellen dienen, u. A., zu einer analytischen Disciplin vom höchsten Interesse gestempelt wird. Dies Gebiet hat zugleich das Charakteristische, dass in ihm die geometrische Bedeutung der quadratischen Formen als Punkt- oder Zahlengitter vorzüglich zur Geltung kommt. Der letzte Abschnitt des Werkes wird der zusammenhängenden Darstellung der betreffenden Arbeiten vornehmlich von Hermite, dann Selling und Charve, Dirichlet, F. Klein, Poincaré, Minkowski u. A. gewidmet sein.

Die Menge und der Umfang der erforderlichen oder in Frage kommenden Untersuchungen, zugleich mit dem Umstande, dass sowohl die zwei ersten Abschnitte zusammengenommen, wie auch der dritte für sich als ein in sich abgeschlossenes Ganzes angesehen werden dürfen, rechtfertigt es, wenn hier zunächst nur die ersteren beiden als erste Abtheilung des ganzen vierten Theiles meiner Zahlentheorie veröffentlicht werden. Die zweite Abtheilung, an deren Vollendung ausser sonstigen Umständen zur Zeit noch andere nothwendige Arbeiten mich verhindern, soll, sobald es mir möglich sein wird, dieser ersten Abtheilung nachfolgen. —

Weimar, den 20. Mai 1898.

Inhaltsverzeichniss.

Drittes Capitel.

Von der Darstellung durch eine gegebene Form.

Viertes Capitel.

Die ganzzahligen Transformationen einer ternären quadratischen Form in sich selbst.

Fünftes Capitel.

Vom Vorhandensein der Geschlechter.

Sechstes Capitel.

Positive Formen. Die Form $x^2 + x'^2 + x''^2$.

Siebentes Capitel.

Bestimmung des Maasses eines Geschlechts und einer Ordnung positiver Formen.

Achtes Capitel.

Unbestimmte Formen. Die Gleichung $ax^2 + a'x'^2 + a''x''^2 = 0$.

Neuntes Capitel.

Unbestimmte Formen. Classenzahl eines Geschlechts.

Zweiter Abschnitt.

Die allgemeinen quadratischen Formen.

Erstes Capitel.

Algebraische Hilfssätze.

Zweites Capitel.

Von den Elementartheilern der Zahlensysteme.

Drittes Capitel.
Die linearen Gleichungen.

Viertes Capitel.
Die linearen Congruenzen.

Fünftes Capitel.
Algebraisches über quadratische Formen.

Sechstes Capitel.

Classen, Ordnungen, Geschlechter quadratischer Formen.

Siebentes Capitel.

Ueber quadratische Congruenzen.

Achtes Capitel.

Neue Definition des Geschlechts.

Neuntes Capitel.

Die Darstellung durch eine quadratische Form.

Zehntes Capitel.

Positive Formen. Vom Maasse derselben.

Einleitung.

Nachdem Gauss in den Disquisitiones Arithmeticae die Theorie der binären quadratischen Formen zuerst in systematisch folgerechter und umfassender Weise zur Darstellung gebracht, weist er in art. 266 den Mathematikern ein weites, unermessliches Gebiet zu ähnlicher Forschung: die arithmetische Untersuchung der homogenen ganzen Funktionen beliebigen Grades und mit einer beliebigen Anzahl von Veränderlichen, ein Gebiet, von welchem die von ihm entwickelte Theorie der binären quadratischen Formen nur die erste, nächstliegende Stufe ist. Sehen wir ab von den binären Formen eines beliebigen Grades > 2, deren Arithmetik seither nur in sehr geringem Umfange behandelt worden ist*), so zeichnen sich unter den übrigen Formen oder homogenen Funktionen zwei Kategorieen besonders aus: die zerlegbaren Formen, d. h. diejenigen Formen n^{ten} Grades, welche als Produkte von n irrationalen Faktoren ersten Grades darstellbar sind, und die allgemeinen quadratischen Formen mit einer beliebigen Anzahl n von Variabeln. Die binären quadratischen Formen sind unter allen Formen durch den besonderen Umstand charakterisirt, dass sie diesen beiden Kategorieen von Formen zugleich angehörig sind. Zahlentheoretisch betrachtet, kommt der erstern von beiden bei weitem grössere Wichtigkeit und höheres Interesse zu, denn unter der algebraischen Form

*) S. darüber Eisenstein, théorèmes sur les formes cubiques et solution d'une équation du quatrième degré à quatre indéterminées, sowie „Untersuchungen über die kubischen Formen mit zwei Variabeln" im Journal für Mathematik 27; desgl. Hermite, sur la théorie des fonctions homogènes à deux indéterminées, ebendas. Bd. 52.

verbirgt sich bei ihnen ein wesentlich arithmetischer Kern: die allgemeine complexe oder algebraische ganze Zahl, deren Eigenschaften im arithmetischen Verhalten jener Formen zu formalem Ausdrucke gelangen. Aus diesem Grunde schien es uns bei unserer Darstellung der Lehre von den binären quadratischen Formen*) vom zahlentheoretischen Standpunkte geboten, thunlichst alles aus rein arithmetischen Quellen abzuleiten und algebraische Hilfsmittel nach Möglichkeit zu vermeiden; in einem späteren Theile unsers Unternehmens, in der Theorie der algebraischen ganzen Zahlen soll noch einmal jene Lehre aufgenommen und in der Weise dargestellt werden, dass aus der algebraischen Form der arithmetische Kern völlig herausgeschält erscheine; hier wird sie, als bereits in den Elementen ausreichend behandelt, nur mehr gelegentlich zur Berücksichtigung kommen und mancherlei Ergänzungen erfahren.

Anders als mit den binären verhält es sich mit den quadratischen Formen mit mehr als zwei Veränderlichen. Hier wird es mehr die algebraische Form, welche anzieht, wie herrscht, und es dürfte weder möglich noch sachlich begründet sein, die Arithmetik dieser Formen frei von algebraischen Hilfsmitteln und Gesichtspunkten zu begründen. Wir werden vielmehr, um für die quadratischen Formen mit einer beliebigen Anzahl von Veränderlichen jene zu entwickeln, einer ziemlich breiten algebraischen Grundlage durchaus bedürfen.

Die ersten Untersuchungen über diese Formen datiren von Euler und Lagrange und knüpfen sich an die Aufgabe, die allgemeine Gleichung zweiten Grades

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

in ganzen oder rationalen Zahlen zu lösen. Legendre entwickelte sodann an der besonderen ternären quadratischen Form

$$x^2 + y^2 + z^2$$

bereits, wenn auch unter anderer Fassung, die gleichen Gesichtspunkte, welche nach Gauss' digressio continens tractatum de formis ternariis seiner Disqu. Arithm. art. 266—285 die Arithmetik dieser Formen beherrschen und denjenigen, die

*) Elemente der Zahlentheorie, Leipzig, 1892.

in der Lehre von den binären quadratischen Formen ausreichend sind, sich hinzugesellen. Gauss hat jedoch die Theorie der ternären quadratischen Formen nur soweit entwickelt, als er ihrer bedurfte, um seine Lehre von den binären zu krönen, indem er vermittelst jener den Nachweis lieferte, dass die für eine bestimmte Determinante zulässigen Geschlechter solcher Formen wirklich vorhanden sind. Den nächsten Fortschritt in jener Theorie verdankt man Seeber*), welcher auf strengem, wenn auch ausserordentlich umständlichem Wege den Beweis gab, dass es in jeder Classe positiver ternärer Formen eine einzige Form gebe, deren Coefficienten gewisse von ihm angegebene Ungleichheitsbedingungen erfüllen. Diese Form heisst nach Gauss' Vorgange die reducirte Form der Classe. Gleichzeitig richtete diese Arbeit die Aufmerksamkeit auf die geometrische Bedeutung der positiven binären wie ternären quadratischen Formen als „Zahlengitter“ und, solcher Auffassung sich bemächtigend, war es nun Dirichlet, welcher in einer klassisch schönen Arbeit die Seeber'schen Reduktionsbedingungen auf die einfachste Art ableitete. Hermite förderte sodann die algebraischen Grundlagen der Theorie durch Aufstellung aller Transformationen einer ternären quadratischen Form in sich selbst. Noch bedeutend wichtiger aber wurden seine Untersuchungen über die Reduktion der quadratischen Formen. Indem er dieselbe auf die Betrachtung stetig veränderlicher Elemente, die er einführte, begründete, andererseits aber auf die Eigenschaften der positiven quadratischen Formen die Theorie aller andern quadratischen sowie diejenige der zerlegbaren Formen zurückführte, schuf er ein eigenthümliches Gebiet der Zahlentheorie, in welchem sie sich mit der Analysis, wie auch mit geometrischen Theorieen auf das Innigste berührt, und welches dann durch die Forschungen anderer Mathematiker, wie Selling und neuestens ganz besonders Minkowski, einen bedeutenden Umfang erlangt hat.

Wenn mit dieser Hermite'schen Richtung die Theorie der quadratischen Formen mehr allgemein-arithmetischen, ana-

*) L. A. Seeber, Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen, Freiburg i. Br. 1831.

lytisch wichtigen Zielen sich zuwandte, so war es Eisenstein, welcher jene Theorie nach der rein zahlentheoretischen Seite hin durch Einführung dreier neuen fundamentalen Begriffe auf das wesentlichste förderte: der Begriffe der Ordnung, des Geschlechts und ihres Maasses. Seine Formeln für das Maass eines Geschlechts oder einer Ordnung sind später von St. Smith in einer vortrefflichen Abhandlung bewiesen und verallgemeinert worden. Zudem verdankt man letzterem, zu frühe verstorbenen ausgezeichneten Mathematiker eine Reihe von Noten, in denen er Eisensteins Untersuchungen über ternäre Formen auf solche mit beliebig viel Veränderlichen ausdehnt; seine letzte, von der Pariser Akademie preisgekrönte Arbeit über den gleichen Gegenstand lässt einigermassen erkennen, wie die kurzen Angaben jener Noten auszuführen und zu begründen sind. Mit seiner Arbeit zugleich gekrönt wurde eine solche von Minkowski, welche in vielfacher Uebereinstimmung, doch über jene hinausgehend, denselben Gegenstand behandelt, und andere Arbeiten desselben Verfassers haben zusammen mit denen von Smith der Arithmetik der allgemeinen quadratischen Formen bereits solche Ausbildung verliehen, dass, soviel Punkte auch noch zu erledigen bleiben, doch schon ihre einheitliche Darstellung versucht werden kann.

Dies soll nun im Folgenden geschehen und zwar in der Weise, dass zuerst, gleichsam als Paradigma, die einfachere Theorie der ternären quadratischen Formen und in möglichster Abrundung die mannigfachen besonderen auf sie bezüglichen Untersuchungen dargestellt und dann, wenn hierdurch der Leser auf die viel schwierigeren Verhältnisse in der allgemeinen Theorie vorbereitet worden, diese letztere, die Arithmetik der allgemeinen quadratischen Formen entwickelt wird.

Ein letzter Abschnitt — in der zweiten Abtheilung dieses Werkes — soll dem zuvor erwähnten eigenthümlichen Gebiete der Zahlentheorie, das man zahlentheoretische Analysis nennen könnte, gewidmet sein und Alles zusammenfassen, was die Reduktion der quadratischen Formen betrifft und auf derselben begründet ist.

ERSTER ABSCHNITT.

DIE
TERNÄREN QUADRATISCHEN FORMEN.



Erstes Capitel.

Die algebraischen Grundformeln.

1. Wir beginnen also unsere Darstellung mit der Lehre von den ternären quadratischen Formen und entwickeln vor allem ihre algebraische Grundlage. Diese finden wir aber ausser in der linearen Transformation der Formen in den paar folgenden einfachen algebraischen Beziehungen.

Unter einer ternären quadratischen Form verstehen wir jede homogene ganze Funktion zweiten Grades von drei Veränderlichen oder Unbestimmten x, x', x'':

$$(1)\quad \begin{cases} f(x, x', x'') \\ = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx'. \end{cases}$$

Wo es sich nicht darum handelt, ihre Unbestimmten namhaft zu machen, stellt man sie kürzer auch durch das Symbol

$$f(x, x', x'') = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

dar. Ferner setzen wir

$$(2)\quad \begin{cases} f^0(x) = \frac{1}{2}\frac{\partial f}{\partial x} = ax + b''x' + b'x'' \\ f^1(x) = \frac{1}{2}\frac{\partial f}{\partial x'} = b''x + a'x' + bx'' \\ f^2(x) = \frac{1}{2}\frac{\partial f}{\partial x''} = b'x + bx' + a''x''. \end{cases}$$

Alsdann besteht die Gleichung

$$(3)\quad f(x, x', x'') = f^0(x) . x + f^1(x) \cdot x' + f^2(x) \cdot x''.$$

Führt man nun durch die Gleichungen

$$(4)\quad \begin{cases} X = ax + b''x' + b'x'', \quad X' = b''x + a'x' + bx'', \\ \qquad X'' = b'x + bx' + a''x'' \end{cases}$$

drei neue Veränderliche X, X', X'' ein, so soll die Determinante dieser Gleichungen:

$$(5)\qquad D = \begin{vmatrix} a & b'' & b' \\ b'' & a' & b \\ b' & b & a'' \end{vmatrix}$$

nach Gauss' Vorgange (der jedoch die Determinante mit entgegengesetztem Vorzeichen nimmt) auch die Determinante der Form (1) heissen. Ihr entwickelter Ausdruck ist

$$(5\text{a})\qquad D = aa'a'' + 2bb'b'' - ab^2 - a'b'^2 - a''b''^2$$

und es bestehen folgende Beziehungen:

$$(6)\quad \left\{\begin{array}{ll} aA + b''B'' + b'B' = D, & aB'' + b''A' + b'B = 0, \\ & aB' + b''B + b'A'' = 0 \\ b''A + a'B'' + bB' = 0, & b''B'' + a'A' + bB = D, \\ & b''B' + a'B + bA'' = 0 \\ b'A + bB'' + a''B' = 0, & b'B'' + bA' + a''B = 0, \\ & b'B' + bB + a''A'' = D \end{array}\right.$$

zwischen den Elementen der Determinante D und den ihnen entsprechenden Elementen der adjungirten Determinante

$$(7)\quad \mathrm{D} = \begin{vmatrix} A = a'a'' - b^2, & B'' = bb' - a''b'', & B' = b''b - a'b' \\ B'' = bb' - a''b'', & A' = a''a - b'^2, & B = b'b'' - ab \\ B' = b''b - a'b', & B = b'b'' - ab, & A'' = aa' - b''^2 \end{vmatrix}.$$

Vermittelst derselben ergeben sich, wenn

$$(8)\qquad Dx = \xi,\quad Dx' = \xi',\quad Dx'' = \xi''$$

gesetzt wird, aus (4) die umgekehrten Gleichungen

$$(9)\quad \left\{\begin{array}{ll} \xi = AX + B''X' + B'X'', & \xi' = B''X + A'X' + BX'', \\ & \xi'' = B'X + BX' + A''X'' \end{array}\right.$$

sowie aus (6) gemäss dem Multiplikationssatze der Determinanten zwischen D, D folgende Beziehung:

$$D \cdot \mathrm{D} = D^3$$

d. h., wenn, wie es allgemein geschehen soll, die Determinante D der Form als von Null verschieden vorausgesetzt wird,

$$(10)\qquad \mathrm{D} = D^2.$$

Mit Rücksicht auf (3) aber kann man schreiben:

$$D \cdot f(x, x', x'') = D(Xx + X'x' + X''x'')$$

und diese Gleichung führt vermittelst der Gleichungen (8) und (9) sofort zur Beziehung:

$$D \cdot f(x, x', x'') = F(X, X', X''), \tag{11}$$

wenn unter $F(X, X', X'')$ die ternäre Form

$$\begin{cases} AX^2 + A'X'^2 + A''X''^2 \\ \qquad + 2BX'X'' + 2B'X''X + 2B''XX' \end{cases} \tag{12}$$

verstanden wird; man nennt diese letztere die zu f adjungirte Form.

Nun stehen aber die Gleichungen (9) in genau derselben Beziehung zur Form F, wie die Gleichungen (4) zur Form f. Nennt man demnach φ die adjungirte Form zur Adjungirten F, so wird man auch die mit (11) analoge Gleichung

$$\mathrm{D} \cdot F(X, X', X'') = \varphi(\xi, \xi', \xi'')$$

schreiben dürfen, welche mit Rücksicht auf (8) und (10) und auf die Homogeneität der quadratischen Form φ sogleich in die folgende

$$F(X, X', X'') = \varphi(x, x', x'')$$

oder wegen (11) auch in diese andere:

$$\varphi(x, x', x'') = D \cdot f(x, x', x'') \tag{13}$$

sich verwandeln lässt.

Man erhält mit andern Worten die Adjungirte der adjungirten Form aus der ursprünglich gegebenen Form einfach dadurch, dass man diese mit ihrer Determinante multiplicirt. Und hiernach werden nachstehende Beziehungen stattfinden müssen:

$$\begin{cases} A'A'' - B^2 = Da, & A''A - B'^2 = Da', \\ & AA' - B''^2 = Da'', \\ B'B'' - AB = Db, & B''B - A'B' = Db', \\ & BB' - A''B'' = Db''.\text{*)} \end{cases} \tag{14}$$

---

*) Auf ähnliche Weise, wie hier geschehen, leitet Biehler (Nouv. Ann. (3) 6, S. 79) dieselben Beziehungen her.

2. Hier sei an eine bekannte Formel der Determinantentheorie erinnert, nach welcher die Determinante

$$(15)\quad \begin{vmatrix} a\alpha + a'\alpha' + a''\alpha'', & a\beta + a'\beta' + a''\beta'' \\ b\alpha + b'\alpha' + b''\alpha'', & b\beta + b'\beta' + b''\beta'' \end{vmatrix} = \begin{vmatrix} a', a'' \\ b', b'' \end{vmatrix} \cdot \begin{vmatrix} \alpha', \alpha'' \\ \beta', \beta'' \end{vmatrix} + \begin{vmatrix} a'', a \\ b'', b \end{vmatrix} \cdot \begin{vmatrix} \alpha'', \alpha \\ \beta'', \beta \end{vmatrix} + \begin{vmatrix} a, a' \\ b, b' \end{vmatrix} \cdot \begin{vmatrix} \alpha, \alpha' \\ \beta, \beta' \end{vmatrix}$$

ist. In Anwendung dieser Formel findet man, wenn y, y', y'' drei neue Unbestimmte bezeichnen, diese drei Gleichungen:

$$\begin{vmatrix} f^1(x), f^2(x) \\ f^1(y), f^2(y) \end{vmatrix} = A(x'y'' - x''y') + B''(x''y - xy'') + B'(xy' - x'y)$$

$$\begin{vmatrix} f^2(x), f^0(x) \\ f^2(y), f^0(y) \end{vmatrix} = B''(x'y'' - x''y') + A'(x''y - xy'') + B(xy' - x'y)$$

$$\begin{vmatrix} f^0(x), f^1(x) \\ f^0(y), f^1(y) \end{vmatrix} = B'(x'y'' - x''y') + B(x''y - xy'') + A''(xy' - x'y).$$

Wenn daher nun dieselbe Hilfsformel benutzt wird, um die Determinante

$$\begin{vmatrix} f^0(x)\cdot x + f^1(x)\cdot x' + f^2(x)\cdot x'', & f^0(x)\cdot y + f^1(x)\cdot y' + f^2(x)\cdot y'' \\ f^0(y)\cdot x + f^1(y)\cdot x' + f^2(y)\cdot x'', & f^0(y)\cdot y + f^1(y)\cdot y' + f^2(y)\cdot y'' \end{vmatrix}$$

zu entwickeln, so geht durch Substitution der soeben gefundenen Werthe und mit Berücksichtigung der einfachen Beziehung

$$(16)\quad f^0(y)\cdot x + f^1(y)\cdot x' + f^2(y)\cdot x'' = f^0(x)\cdot y + f^1(x)\cdot y' + f^2(x)\cdot y''$$

nachstehende Formel hervor:

$$(17)\quad f(x,x',x'')\cdot f(y,y',y'') - (f^0(y)\cdot x + f^1(y)\cdot x' + f^2(y)\cdot x'')^2 = F(x'y'' - x''y',\ x''y - xy'',\ xy' - x'y).$$

Die entsprechende Formel für die adjungirte Form F erhält mit Beachtung von (13) die Gestalt:

$$(18)\quad F(x,x',x'')\cdot F(y,y',y'') - (F^0(y)\cdot x + F^1(y)\cdot x' + F^2(y)\cdot x'')^2 = D\cdot f(x'y'' - x''y',\ x''y - xy'',\ xy' - x'y).$$

Diese so gewonnenen beiden Formeln (17) und (18) sind in solchem Grade für alles Folgende als

Grundlage anzusehen, dass wir sie geradezu als *die beiden Grundformeln* bezeichnen werden.

Diese Grundformeln führen zunächst zur Unterscheidung aller ternären quadratischen Formen in zwei Arten: in die bestimmten und die unbestimmten Formen. Die erstern Formen erhalten, wenn für die Unbestimmten darin alle möglichen Werthe gesetzt werden, die nicht gleichzeitig Null sind, nur Werthe eines bestimmten Vorzeichens und werden dann je nach diesem Vorzeichen positive oder negative Formen genannt. Die andern aber vermögen gleicherweise positive wie negative Werthe anzunehmen; zu ihnen zählen auch diejenigen Formen, welche den Werth Null erhalten können (Nullformen), ohne dass sämmtliche Unbestimmte gleich Null gewählt werden.

Soll eine Form f eine bestimmte sein, so müssen jedenfalls die drei Coefficienten a, a', a'', die auch Werthe der Form sind, von Null verschieden sein. Nach den Gleichungen (4) entsprechen aber Werthen der Unbestimmten x, x', x'', welche nicht gleichzeitig verschwinden, auch solche Werthe von X, X', X'' und umgekehrt; demnach lehrt die Gleichung (11) sofort, dass eine Form f und ihre Adjungirte F stets gleichzeitig bestimmte bezw. gleichzeitig unbestimmte Formen sein werden. Also müssen, damit f eine bestimmte Form sei, auch A, A', A'' von Null verschieden sein. Nun folgert man aus der ersten Grundformel für $y = 1$, $y' = y'' = 0$ die folgende:

$$a \cdot f(x, x', x'') = (ax + b''x' + b'x'')^2 + A'x''^2 - 2Bx'x'' + A''x'^2,$$

aus welcher diese andere:

$$aA' \cdot f(x, x', x'') = A'(ax + b''x' + b'x'')^2 + (A'x'' - Bx')^2 + Dax'^2$$

hervorgeht, die wieder, indem man

$$ax + b''x' + b'x'' = \xi, \quad A'x'' - Bx' = \xi', \ x' = \xi''$$

setzt, die neue Gestalt annimmt:

$$aA' \cdot f(x, x', x'') = A'\xi^2 + \xi'^2 + Da\xi''^2.$$

Jedem von Null verschiedenen Systeme ξ, ξ', ξ'' entspricht nach der voraufgehenden Substitution ein ebensolches System

x, x', x''. Soll daher f bestimmt sein, so müssen A' und Da positiv sein, denn sonst würde

$$aA' \cdot f(x, x', x'')$$

positiv, wenn x, x', x'' der Annahme $\xi = 0$, $\xi'' = 0$ gemäss, dagegen negativ, wenn sie so gewählt werden, dass diejenigen Werthe ξ, ξ', ξ'' verschwinden, welche dem einen oder den zwei positiven Coefficienten entsprechen. Umgekehrt leuchtet ein, dass, wenn A', Da positiv sind, $f(x, x', x'')$ nur solche Werthe annehmen kann, die dasselbe Vorzeichen haben wie aA' d. h. wie a. — Hier war indessen die Wahl der beiden Coefficienten a, A' willkürlich unter den möglichen Combinationen der Coefficienten a, a', a'' einer- und der Coefficienten A, A', A'' andererseits. Man erhält demnach schliesslich folgendes Resultat:

Damit $f(x, x', x'')$ eine bestimmte Form sei, ist nothwendig und hinreichend, dass die Grössen

$$A,\ A',\ A'',\ Da,\ Da',\ Da''$$

positiv sind; und je nachdem a, a', a'' positiv oder negativ sind, wird die Form dann eine positive oder eine negative sein.

Jede negative Form entsteht offenbar aus einer positiven, indem man diese mit -1 multiplicirt; es ist daher überflüssig, negative Formen einer besonderen Betrachtung zu unterziehen, und wir dürfen uns in der Folge bei Betrachtung bestimmter Formen auf die positiven beschränken. In gleicher Weise schliessen wir bei den unbestimmten diejenigen mit negativer Determinante vollständig aus, da sie sich aus solchen mit positiver Determinante durch Multiplikation mit -1 ergeben.

3. Im Anschluss an die beiden Grundformeln soll hier sogleich der quaternären quadratischen Form

$$\xi^2 + F(x, x', x'')$$

Erwähnung geschehen, um eine Eigenschaft derselben herzuleiten, welche für unsere Theorie wesentlich ist: Diese Form reproducirt sich durch Multiplikation. Man giebt nämlich leicht mittels der zweiten Grundformel dem Produkte

$$(\xi^2 + F(x, x', x''))\,(\eta^2 + F(y, y', y''))$$

die Form

$$[\xi\eta - xF^0(y) - x'F^1(y) - x''F^2(y)]^2$$
$$+ F(\eta x + \xi y,\ \eta x' + \xi y',\ \eta x'' + \xi y'') + D \cdot f(s, s', s''),$$

wo

$$(19)\qquad s = x'y'' - x''y',\quad s' = x''y - xy'',\quad s'' = xy' - x'y$$

gesetzt ist. Die beiden letzten Glieder kann man jedoch in die Form

$$F(\eta x + \xi y + t,\quad \eta x' + \xi y' + t',\quad \eta x'' + \xi y'' + t'')$$

zusammenziehen, wenn man t, t', t'' so bestimmt, dass die Gleichung

$$\begin{aligned}(2\eta x + 2\xi y + t)\,F^0(t) + (2\eta x' + 2\xi y' + t')\,F^1(t)\\ + (2\eta x'' + 2\xi y'' + t'')F^2(t)\\ = D \cdot f(s, s', s'')\end{aligned}$$

erfüllt wird; letzteres geschieht für

$$t = f^0(s),\quad t' = f^1(s),\quad t'' = f^2(s),$$

wodurch

$$F^0(t) = Ds,\quad F^1(t) = Ds',\quad F^2(t) = Ds''$$

wird, während andererseits

$$xs + x's' + x''s'' = 0,\quad ys + y's' + y''s'' = 0$$

ist. — Auf solche Weise stellt sich folgende Gleichung heraus:

$$(20)\qquad (\xi^2 + F(x, x', x''))\cdot(\eta^2 + F(y, y', y'')) = \zeta^2 + F(z, z', z''),$$

in welcher

$$(21)\qquad \begin{cases}\zeta = \xi\eta - xF^0(y) - x'F^1(y) - x''F^2(y)\\ z = \eta x + \xi y + f^0(s)\\ z' = \eta x' + \xi y' + f^1(s)\\ z'' = \eta x'' + \xi y'' + f^2(s)\end{cases}$$

zu setzen ist.

Einfache Fälle dieser merkwürdigen Gleichung gaben bereits Euler und Lagrange*). Versteht man nämlich unter f die Form $-x^2 - x'^2 - x''^2$, so ist

$$F = x^2 + x'^2 + x''^2$$

---

*) S. dazu Lagrange's Abh. in den Mém. de l'Acad. de Berlin, 1770, sowie Euler, comment. arithm. coll. I S. 543.

und die Formeln (20) und (21) ergeben

$$(22)\quad \begin{cases} (\xi^2+x^2+x'^2+x''^2)\cdot(\eta^2+y^2+y'^2+y''^2) \\ =(\xi\eta-xy-x'y'-x''y'')^2+(\eta x+\xi y-x'y''+x''y')^2 \\ +(\eta x'+\xi y'-x''y+xy'')^2+(\eta x''+\xi y''-xy'+x'y)^2. \end{cases}$$

Dies ist die Formel von Euler, nach welcher eine Summe von vier Quadraten mit einer zweiten solchen Summe multiplicirt wieder eine Summe von vier Quadraten ist. Da man sowohl die Grössen ξ, x, x', x'' unter sich und die Grössen η, y, y', y'' unter einander vertauschen als auch mit entgegengesetzten Vorzeichen nehmen darf, lässt sich das Produkt auf mannigfaltige Weise wieder in der Quadratsummen-Form der Faktoren zur Darstellung bringen.

Versteht man dagegen unter f die Form $-Cx^2-Bx'^2+x''^2$, so wird F die Form $-Bx^2-Cx'^2+BCx''^2$ und die Formeln (20) und (21) führen zu der Gleichung von Lagrange:

$$(23)\quad \begin{cases} (\xi^2-Bx^2-Cx'^2+BCx''^2)\cdot(\eta^2-By^2-Cy'^2+BCy''^2) \\ =(\xi\eta+Bxy+Cx'y'-BCx''y'')^2 \\ -B\cdot(\eta x+\xi y-C(x'y''-x''y'))^2 \\ -C\cdot(\eta x'+\xi y'-B(x''y-xy''))^2 \\ +BC\cdot(\eta x''+\xi y''+xy'-x'y)^2, \end{cases}$$

deren rechte Seite sich ebenfalls mannigfach verändern lässt, da jede der Zahlen x, x', x'', y, y', y'' mit entgegengesetztem Vorzeichen gewählt werden darf.

Die lineare Transformation.

4. Eine weitere Grundlage unserer Lehre von den quadratischen Formen ist ihre Transformation durch lineare Substitutionen. Macht man in der ternären quadratischen Form $f(x, x', x'')$ eine solche Substitution:

$$(24)\quad \begin{cases} x\ =\alpha_0{}^0 y+\alpha_0{}' y'+\alpha_0{}'' y'' \\ x'\ =\alpha_1{}^0 y+\alpha_1{}' y'+\alpha_1{}'' y'' \\ x''=\alpha_2{}^0 y+\alpha_2{}' y'+\alpha_2{}'' y'', \end{cases}$$

deren Determinante — der sogenannte Modulus der Substitution — welche A heisse, stets von Null verschieden

vorausgesetzt wird, so verwandelt sich, da bei Anwendung der Abkürzungen

$$(25)\qquad \begin{cases} f_i = f(\alpha_0^{(i)}, \alpha_1^{(i)}, \alpha_2^{(i)}) \\ f_i^k = \frac{1}{2}\frac{\partial f_i}{\partial \alpha_k^{(i)}} \end{cases}$$

die allgemeine Beziehung

$$(26)\qquad f^k(x) = f_0^k \cdot y + f_1^k \cdot y' + f_2^k \cdot y''$$

gefunden wird, wegen (3) die quadratische Form $f(x, x', x'')$ in eine andere ternäre quadratische Form

$$f_1(y, y', y'') = a_1 y^2 + a_1' y'^2 + a_1'' y''^2 + 2b_1 y' y'' + 2b_1' y'' y + 2b_1'' y y',$$

deren Coefficienten mit denjenigen der ersteren Form durch nachstehende Gleichungen verbunden sind:

$$(27)\qquad \begin{cases} a_1 = f_0^0 \cdot \alpha_0^0 + f_0^1 \cdot \alpha_1^0 + f_0^2 \cdot \alpha_2^0 = f_0\,. \\ a_1' = f_1^0 \cdot \alpha_0' + f_1^1 \cdot \alpha_1' + f_1^2 \cdot \alpha_2' = f_1 \\ a_1'' = f_2^0 \cdot \alpha_0'' + f_2^1 \cdot \alpha_1'' + f_2^2 \cdot \alpha_2'' = f_2 \\ b_1 = f_1^0 \cdot \alpha_0'' + f_1^1 \cdot \alpha_1'' + f_1^2 \cdot \alpha_2'' = f_2^0 \cdot \alpha_0' + f_2^1 \cdot \alpha_1' + f_2^2 \cdot \alpha_2' \\ b_1' = f_2^0 \cdot \alpha_0^0 + f_2^1 \cdot \alpha_1^0 + f_2^2 \cdot \alpha_2^0 = f_0^0 \cdot \alpha_0'' + f_0^1 \cdot \alpha_1'' + f_0^2 \cdot \alpha_2'' \\ b_1'' = f_0^0 \cdot \alpha_0' + f_0^1 \cdot \alpha_1' + f_0^2 \cdot \alpha_2' = f_1^0 \cdot \alpha_0^0 + f_1^1 \cdot \alpha_1^0 + f_1^2 \cdot \alpha_2^0. \end{cases}$$

In Folge derselben ist die Determinante

$$D_1 = \begin{vmatrix} a_1, & b_1'', & b_1' \\ b_1'', & a_1', & b_1 \\ b_1', & b_1, & a_1'' \end{vmatrix}$$

gleich dem Produkte

$$\begin{vmatrix} f_0^0, & f_0^1, & f_0^2 \\ f_1^0, & f_1^1, & f_1^2 \\ f_2^0, & f_2^1, & f_2^2 \end{vmatrix} \cdot \begin{vmatrix} \alpha_0^0, & \alpha_1^0, & \alpha_2^0 \\ \alpha_0', & \alpha_1', & \alpha_2' \\ \alpha_0'', & \alpha_1'', & \alpha_2'' \end{vmatrix} = \begin{vmatrix} a, & b'', & b' \\ b'', & a', & b \\ b', & b, & a'' \end{vmatrix} \cdot \begin{vmatrix} \alpha_0^0, & \alpha_1^0, & \alpha_2^0 \\ \alpha_0', & \alpha_1', & \alpha_2' \\ \alpha_0'', & \alpha_1'', & \alpha_2'' \end{vmatrix}^2$$

d. h. zwischen den Determinanten D, D_1 der ursprünglichen und der transformirten quadratischen Form besteht die Beziehung

$$(28)\qquad D_1 = D \cdot \mathsf{A}^2.$$

Durch Auflösung der Gleichungen (24) erhält man

$$(29)\quad \begin{cases} \mathsf{A}\cdot y \;\;= \mathsf{A}_0{}^0 x + \mathsf{A}_1{}^0 x' + \mathsf{A}_2{}^0 x'' \\ \mathsf{A}\cdot y' \;= \mathsf{A}_0{}' x + \mathsf{A}_1{}' x' + \mathsf{A}_2{}' x'' \\ \mathsf{A}\cdot y'' = \mathsf{A}_0{}'' x + \mathsf{A}_1{}'' x' + \mathsf{A}_2{}'' x'', \end{cases}$$

worin

$$(30)\quad \begin{cases} \mathsf{A}_0{}^0 = \alpha_1{}'\alpha_2{}'' - \alpha_1{}''\alpha_2{}', & \mathsf{A}_0{}' = \alpha_1{}''\alpha_2{}^0 - \alpha_1{}^0\alpha_2{}'', \\ & \mathsf{A}_0{}'' = \alpha_1{}^0\alpha_2{}' - \alpha_1{}'\alpha_2{}^0 \\ \mathsf{A}_1{}^0 = \alpha_2{}'\alpha_0{}'' - \alpha_2{}''\alpha_0{}', & \mathsf{A}_1{}' = \alpha_2{}''\alpha_0{}^0 - \alpha_2{}^0\alpha_0{}'', \\ & \mathsf{A}_1{}'' = \alpha_2{}^0\alpha_0{}' - \alpha_2{}'\alpha_0{}^0 \\ \mathsf{A}_2{}^0 = \alpha_0{}'\alpha_1{}'' - \alpha_0{}''\alpha_1{}', & \mathsf{A}_2{}' = \alpha_0{}''\alpha_1{}^0 - \alpha_0{}^0\alpha_1{}'', \\ & \mathsf{A}_2{}'' = \alpha_0{}^0\alpha_1{}' - \alpha_0{}'\alpha_1{}^0 \end{cases}$$

ist. Offenbar kehrt durch die Substitution (29) die Form $f_1(y, y', y'')$ wieder in die Form $f(x, x', x'')$ zurück, weshalb jene die umgekehrte Substitution (24) genannt werden soll.

Setzt man nun analog den Gleichungen (4)

$$(31)\quad \begin{cases} Y \;\;= \frac{1}{2}\frac{\partial f_1}{\partial y} = a_1 y + b_1{}'' y' + b_1{}' y'' \\ Y' \;= \frac{1}{2}\frac{\partial f_1}{\partial y'} = b_1{}'' y + a_1{}' y' + b_1 y'' \\ Y'' = \frac{1}{2}\frac{\partial f_1}{\partial y''} = b_1{}' y + b_1 y' + a_1{}'' y'', \end{cases}$$

so findet sich den Relationen (27) zufolge ohne Mühe

$$Y = f_0{}^0\cdot x + f_0{}^1\cdot x' + f_0{}^2\cdot x'' = f^0(x)\cdot\alpha_0{}^0 + f^1(x)\cdot\alpha_1{}^0 + f^2(x)\cdot\alpha_2{}^0$$

d. i. die erste der folgenden drei Gleichungen, deren beide andere auf entsprechende Weise entstehen:

$$(32)\quad \begin{cases} Y \;\;= \alpha_0{}^0 X + \alpha_1{}^0 X' + \alpha_2{}^0 X'' \\ Y' \;= \alpha_0{}' X + \alpha_1{}' X' + \alpha_2{}' X'' \\ Y'' = \alpha_0{}'' X + \alpha_1{}'' X' + \alpha_2{}'' X''. \end{cases}$$

Umgekehrt erhält man demnach

$$(33)\quad \begin{cases} \mathsf{A}\cdot X \;\;= \mathsf{A}_0{}^0 Y + \mathsf{A}_0{}' Y' + \mathsf{A}_0{}'' Y'' \\ \mathsf{A}\cdot X' \;= \mathsf{A}_1{}^0 Y + \mathsf{A}_1{}' Y' + \mathsf{A}_1{}'' Y'' \\ \mathsf{A}\cdot X'' = \mathsf{A}_2{}^0 Y + \mathsf{A}_2{}' Y' + \mathsf{A}_2{}'' Y''. \end{cases}$$

Nach Gauss bezeichnet man diese Substitutionen (32) und (33) als die transponirten Substitutionen (24) und (29) resp.

Der Gleichung (11) zufolge ist

$$\frac{F(X, X', X'')}{D} = f(x, x', x'').$$

Heisst nun $F_1(Y, Y', Y'')$ die adjungirte Form zu $f_1(y, y', y'')$, so wird in gleicher Weise

$$\frac{F_1(Y, Y', Y'')}{D_1} = f_1(y, y', y'')$$

sein, wenn Y, Y', Y'' durch die Gleichungen (31) mit den y, y', y'' verbunden sind. Aus diesen beiden Formeln aber erschliesst man folgenden Satz:

Geht f in f_1 über durch die Substitution (24), so verwandelt sich $\frac{F}{D}$ in $\frac{F_1}{D_1}$ durch die Substitution (33) und umgekehrt $\frac{F_1}{D_1}$ in $\frac{F}{D}$ durch die zu (24) transponirte Substitution (32).

Man nennt die Formen f und f_1 einander äquivalent, wenn der Modulus der Substitution $\mathsf{A} = \pm 1$ ist, und gewinnt somit aus (28) den Satz: Aequivalente Formen haben gleiche Determinanten, ein Satz, der jedoch nicht umgekehrt werden darf. Dem voraufgehenden Satze aber können wir den wichtigen Zusatz hinzufügen:

Sind die Formen f und f_1 einander äquivalent, so sind es auch ihre Adjungirten F und F_1 und wenn f in f_1 übergeht durch die Substitution (24), so verwandelt sich F_1 in F mittels der transponirten Substitution (32) oder umgekehrt F in F_1 mittels der Substitution

$$(34) \qquad \begin{cases} X = \mathsf{A}_0{}^0 Y + \mathsf{A}_0{}' Y' + \mathsf{A}_0{}'' Y'' \\ X' = \mathsf{A}_1{}^0 Y + \mathsf{A}_1{}' Y' + \mathsf{A}_1{}'' Y'' \\ X'' = \mathsf{A}_2{}^0 Y + \mathsf{A}_2{}' Y' + \mathsf{A}_2{}'' Y''. \text{*)} \end{cases}$$

---

*) Wir wollen nicht unterlassen, an dieser Stelle zu bemerken, wie mittels dieser Beziehungen die beiden Grundformeln bestätigt werden können. Es genügt, dies für die erste derselben zu zeigen. Aus den Formeln (27) folgt

$$a_1 a_1' - b_1''^2 = f(\alpha_0{}^0, \alpha_1{}^0, \alpha_2{}^0) \cdot f(\alpha_0{}', \alpha_1{}', \alpha_2{}') - (f_1{}^0 \alpha_0{}^0 + f_1{}^1 \alpha_1{}^0 + f_1{}^2 \alpha_2{}^0)^2;$$

dieser Ausdruck ist aber der Coefficient des letzten Quadrates in der

5. Im Vorigen ist die Form $f(x, x', x'')$ sowie die Substitution (24) als gegeben gedacht und daraus eine neue Form $f_1(y, y', y'')$ hergeleitet. Man denke umgekehrt die beiden Formen f und f_1 gegeben und versuche die Substitution (24) so zu bestimmen, dass sie die erste in die zweite überführt. In diesem Falle werden die Gleichungen (27), welche zuvor die Coefficienten der neuen Form bestimmten, die Bedingungen aussprechen, welche die gesuchte Transformation zu erfüllen hat. Da somit nur 6 Bedingungsgleichungen vorhanden sind für die 9 Substitutionscoefficienten, so bleiben ihrer drei willkürlich oder, was dasselbe sagt, sie lassen sich alle neun durch drei willkürliche Grössen ausdrücken. Es giebt demnach, allgemein gesagt, dreifach unendlich viel Substitutionen, welche eine gegebene ternäre quadratische Form in eine andere gegebene Form dieser Art überführen.

Sei S_0 eine bestimmte Transformation von f in f_1, und S irgend eine zweite, während S_0' die umgekehrte Substitution S_0 ist. Dann geht offenbar f, wenn man erst die Substitution S anwendet, in f_1, und wenn dann die Substitution S_0' gemacht wird, f_1 wieder in f über, d. h. die aus S und S_0' zusammengesetzte Substitution Σ, in Zeichen $\Sigma = S \cdot S_0'$, ist eine Substitution, welche f in sich selbst verwandelt, und man findet

$$S = \Sigma \cdot S_0. \tag{35}$$

Da diese Formel auch umgekehrt eine Substitution S liefert, durch welche f in f_1 übergeht, sobald man für Σ irgend eine Transformation der Form f in sich selbst wählt, erhält man *sämmtliche* Transformationen der Form f in f_1, wenn man sämmtliche Transformationen von f *in sich selbst* mit *einer* von jenen zusammensetzt. Hat man also eine solche Transformation gefunden, so kommt die Aufgabe, sie sämmtlich zu finden, auf die andere Aufgabe zurück:

Form F_1 und kann, da letztere aus F durch die Substitution (34) hervorgeht, durch

$$F(A_0'', A_1'', A_2'') = F(\alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1', \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2', \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0')$$

ausgedrückt werden.

alle Transformationen von f in sich selbst zu ermitteln.

Der Gleichung (35) zufolge ist $\Sigma' = S_0 \cdot S'$, wenn S' die Umkehrung von S, Σ' die Umkehrung von Σ also gleichzeitig mit Σ jede Transformation von f in sich selbst ist; man findet also jede solche Transformation, indem man eine bestimmte Transformation von f in f_1 mit jeder Transformation von f_1 in f zusammensetzt.

Aus (35) folgt ferner

$$S_0' \cdot S = S_0' \cdot \Sigma \cdot S_0, \tag{36}$$

wo nun nach dem eben Bemerkten zur Linken jede Substitution Σ_1 steht, welche f_1 in sich selbst verwandelt. Da umgekehrt die zur Rechten stehende Substitution ebendasselbe bewirkt, welche Transformation von f in sich selbst auch für Σ gewählt wird, so leuchtet der Satz ein: alle Transformationen einer Form in sich selbst erhält man, wenn man *eine* Transformation der Form in eine bestimmte andere Form mit jeder Transformation dieser letztern in sich selbst und die so entstehende Substitution mit der Umkehrung jener einen Transformation zusammensetzt.

Hermite war der Erste, welcher den allgemeinen Ausdruck der Transformationen einer ternären quadratischen Form in sich selbst gegeben hat*). Seine Herleitung derselben liess jedoch eine Lücke bestehen, welche zuerst der Verfasser, soviel ihm bekannt ist, angemerkt und ausgefüllt hat**), was dann Hermite Anlass gab, auch seinerseits noch einmal darauf zurückzukommen***). Aber schon vor dem Verfasser hat G. Cantor die gleichen Formeln auf einwurfsfreie Weise abgeleitet, indem er sich des

*) In Crelle's Journal f. d. r. u. a. Mathematik Bd. 47 S. 307: Sur la théorie des formes quadratiques ternaires indéfinies, und ebendas. S. 313 Sur la théorie des formes quadratiques.

**) Im J. f. d. r. u. a. Math. Bd. 76: Untersuchungen über quadratische Formen.

***) Im J. f. d. r. u. a. Math. Bd. 78: extrait d'une lettre de Mr. Ch. Hermite à Mr. Borchardt sur la transformation des formes quadratiques ternaires en elles-mêmes.

eben ausgesprochenen Satzes bediente*). Deshalb soll zunächst seine Untersuchung hier — wenigstens in ihren Grundzügen — zur Darstellung gebracht werden.

6. Vorweg sei bemerkt, dass es sich nur darum handelt, die positiven Transformationen einer Form in sich selbst anzugeben d. i. diejenigen, deren Modulus positiv also, nach (28), $\mathsf{A} = +1$ ist; denn, indem man alle Elemente einer Transformation der Form in sich selbst entgegengesetzt nimmt, hört sie offenbar nicht auf, eine solche zu sein, ihr Modulus aber wechselt das Vorzeichen.

Dies vorausgeschickt, bezeichne man mit

$$(37)\qquad \begin{cases} x \;\, = \alpha_0{}^0 z + 2\alpha_0{}' z' + \alpha_0{}'' z'' \\ x' \,= \alpha_1{}^0 z + 2\alpha_1{}' z' + \alpha_1{}'' z'' \\ x'' = \alpha_2{}^0 z + 2\alpha_2{}' z' + \alpha_2{}'' z'' \end{cases}$$

irgend eine Substitution, durch welche die Form $f(x, x', x'')$ in die Form

$$4D(zz'' - z'^2)$$

mit der Determinante $16D^3$ übergeht. Die Bedingungen, welche hierzu von den Substitutionscoefficienten erfüllt sein müssen, haben nach den Formeln (27) folgende Gestalt:

$$(38)\qquad \begin{cases} 0 = f_0{}^0 \cdot \alpha_0{}^0 + f_0{}^1 \cdot \alpha_1{}^0 + f_0{}^2 \cdot \alpha_2{}^0 \\ -D = f_1{}^0 \cdot \alpha_0{}' + f_1{}^1 \cdot \alpha_1{}' + f_1{}^2 \cdot \alpha_2{}' \\ 0 = f_2{}^0 \cdot \alpha_0{}'' + f_2{}^1 \cdot \alpha_1{}'' + f_2{}^2 \cdot \alpha_2{}'' \\ 0 = f_1{}^0 \cdot \alpha_0{}'' + f_1{}^1 \cdot \alpha_1{}'' + f_1{}^2 \cdot \alpha_2{}'' = f_2{}^0 \cdot \alpha_0{}' + f_2{}^1 \cdot \alpha_1{}' + f_2{}^2 \cdot \alpha_2{}' \\ 2D = f_2{}^0 \cdot \alpha_0{}^0 + f_2{}^1 \cdot \alpha_1{}^0 + f_2{}^2 \cdot \alpha_2{}^0 = f_0{}^0 \cdot \alpha_0{}'' + f_0{}^1 \cdot \alpha_1{}'' + f_0{}^2 \cdot \alpha_2{}'' \\ 0 = f_0{}^0 \cdot \alpha_0{}' + f_0{}^1 \cdot \alpha_1{}' + f_0{}^2 \cdot \alpha_2{}' = f_1{}^0 \cdot \alpha_0{}^0 + f_1{}^1 \cdot \alpha_1{}^0 + f_1{}^2 \cdot \alpha_2{}^0. \end{cases}$$

Man nehme zudem an, der Werth des Substitutionsmodulus, welcher der Formel (28) zufolge $\pm 4D$ sein muss, sei $\mathsf{A} = +4D$. Alsdann sieht man nach den Sätzen der nr. 4 leicht ein, dass die Adjungirte $F(X, X', X'')$ durch die Substitution

$$(39)\qquad \begin{cases} X \;\, = \mathsf{A}_0{}^0 Z + 2\mathsf{A}_0{}' Z' + \mathsf{A}_0{}'' Z'' \\ X' \,= \mathsf{A}_1{}^0 Z + 2\mathsf{A}_1{}' Z' + \mathsf{A}_1{}'' Z'' \\ X'' = \mathsf{A}_2{}^0 Z + 2\mathsf{A}_2{}' Z' + \mathsf{A}_2{}'' Z'' \end{cases}$$

*) G. Cantor, de transformatione formarum ternariarum quadraticarum, Halis Saxonum, 1869 (Habilitationsschrift).

in die Form $4D^2(ZZ'' - Z'^2)$ verwandelt wird, wenn man setzt

$$(40)\quad \begin{cases} \mathsf{A}_0^0 = \alpha_1'\alpha_2'' - \alpha_1''\alpha_2', & 2\mathsf{A}_0' = \alpha_1''\alpha_2^0 - \alpha_1^0\alpha_2'', \\ & \mathsf{A}_0'' = \alpha_1^0\alpha_2' - \alpha_1'\alpha_2^0 \\ \mathsf{A}_1^0 = \alpha_2'\alpha_0'' - \alpha_2''\alpha_0', & 2\mathsf{A}_1' = \alpha_2''\alpha_0^0 - \alpha_2^0\alpha_0'', \\ & \mathsf{A}_1'' = \alpha_2^0\alpha_0' - \alpha_2'\alpha_0^0 \\ \mathsf{A}_2^0 = \alpha_0'\alpha_1'' - \alpha_0''\alpha_1', & 2\mathsf{A}_2' = \alpha_0''\alpha_1^0 - \alpha_0^0\alpha_1'', \\ & \mathsf{A}_2'' = \alpha_0^0\alpha_1' - \alpha_0'\alpha_1^0. \end{cases}$$

Multiplicirt man aber die erste, letzte und vorletzte der Gleichungen (38) mit A_0^0, $2\mathsf{A}_0'$, A_0'' resp. und addirt sie dann, so ergiebt sich sogleich die erste der folgenden, deren übrige auf analoge Weise erhalten werden:

$$(41)\quad \begin{cases} \mathsf{A}_0'' = f_0^0, & \mathsf{A}_0' = -f_1^0, & \mathsf{A}_0^0 = f_2^0 \\ \mathsf{A}_1'' = f_0^1, & \mathsf{A}_1' = -f_1^1, & \mathsf{A}_1^0 = f_2^1 \\ \mathsf{A}_2'' = f_0^2, & \mathsf{A}_2' = -f_1^2, & \mathsf{A}_2^0 = f_2^2, \end{cases}$$

und hierdurch nehmen die Gleichungen (37), aufgelöst, nachstehende Gestalt an:

$$(42)\quad \begin{cases} 2Dz = \alpha_0''X + \alpha_1''X' + \alpha_2''X'' \\ 2Dz' = -(\alpha_0'X + \alpha_1'X' + \alpha_2'X'') \\ 2Dz'' = \alpha_0^0X + \alpha_1^0X' + \alpha_2^0X'', \end{cases}$$

wenn wieder

$$X = f^0(x), \quad X' = f^1(x), \quad X'' = f^2(x)$$

gedacht wird. Mit Rücksicht auf die alsdann bestehende Gleichheit

$$F(X, X', X'') = D \cdot f(x, x', x'') = 4D^2(zz'' - z'^2)$$

geht hieraus folgende Gleichung:

$$(43)\quad \begin{cases} F(X, X', X'') = (\alpha_0^0X + \alpha_1^0X' + \alpha_2^0X'') \\ \quad \cdot(\alpha_0''X + \alpha_1''X' + \alpha_2''X'') - (\alpha_0'X + \alpha_1'X' + \alpha_2'X'')^2 \end{cases}$$

hervor, welche identisch besteht und diesem Systeme von Relationen:

$$(44)\quad \begin{cases} A = \alpha_0^0\alpha_0'' - \alpha_0'^2, \quad A' = \alpha_1^0\alpha_1'' - \alpha_1'^2, \quad A'' = \alpha_2^0\alpha_2'' - \alpha_2'^2 \\ 2B = \alpha_1^0\alpha_2'' + \alpha_2^0\alpha_1'' - 2\alpha_1'\alpha_2' \\ 2B' = \alpha_2^0\alpha_0'' + \alpha_0^0\alpha_2'' - 2\alpha_2'\alpha_0' \\ 2B'' = \alpha_0^0\alpha_1'' + \alpha_1^0\alpha_0'' - 2\alpha_0'\alpha_1' \end{cases}$$

gleichbedeutend ist.

Wie aber die voraufgehenden Formeln der Form $f(x, x', x'')$, genau so entsprechen ihrer adjungirten Form die folgenden analogen:

$$(45)\quad \begin{cases} D \cdot f(x, x', x'') = (A_0^0 x + A_1^0 x' + A_2^0 x'') \\ \qquad \cdot (A_0'' x + A_1'' x' + A_2'' x'') - (A_0' x + A_1' x' + A_2' x'')^2 \end{cases}$$

und

$$(46)\quad \begin{cases} Da = A_0^0 A_0'' - A_0'^2,\ Da' = A_1^0 A_1'' - A_1'^2,\ Da'' = A_2^0 A_2'' - A_2'^2 \\ 2Db \ = A_1^0 A_2'' + A_2^0 A_1'' - 2A_1' A_2' \\ 2Db' \ = A_2^0 A_0'' + A_0^0 A_2'' - 2A_2' A_0' \\ 2Db'' = A_0^0 A_1'' + A_1^0 A_0'' - 2A_0' A_1'. \end{cases}$$

An späterer Stelle werden wir auf diese Relationen zurückzuweisen haben.

7. Suchen wir nunmehr die Transformationen der quadratischen Form

$$zz'' - z'^2$$

in sich selbst. Damit

$$(47)\quad \begin{cases} z \ = \lambda\zeta + \mu\zeta' + \nu\zeta'' \\ z' \ = \lambda'\zeta + \mu'\zeta' + \nu'\zeta'' \\ z'' = \lambda''\zeta + \mu''\zeta' + \nu''\zeta'' \end{cases}$$

eine solche sei, muss identisch

$$\zeta\zeta'' - \zeta'^2 = (\lambda\zeta + \mu\zeta' + \nu\zeta'')(\lambda''\zeta + \mu''\zeta' + \nu''\zeta'') - (\lambda'\zeta + \mu'\zeta' + \nu'\zeta'')^2$$

also folgende Gleichungen erfüllt sein:

$$0 = \lambda'^2 - \lambda\lambda'', \quad 1 = \mu'^2 - \mu\mu'', \quad 0 = \nu'^2 - \nu\nu''$$
$$0 = \mu\nu'' + \mu''\nu - 2\mu'\nu', \quad 1 = \lambda\nu'' + \lambda''\nu - 2\lambda'\nu',$$
$$0 = \lambda''\mu + \lambda\mu'' - 2\lambda'\mu'.$$

Führt man nun durch die Gleichungen

$$\lambda = p^2, \quad \nu = q^2, \quad \lambda'' = r^2, \quad \nu'' = s^2$$

vier andere Grössen p, q, r, s ein, so ergiebt sich aus den vorigen Beziehungen bei passender Wahl der Vorzeichen von p und q

$$\lambda' = pr, \quad \nu' = qs;$$

die vorletzte der Beziehungen aber nimmt die Gestalt

$$(ps - qr)^2 = 1$$

an und giebt bei passender Wahl der Vorzeichen von r und s

$$ps - qr = +1.$$

Schreibt man ferner die 4. und 6. der Beziehungen in folgender Weise:

$$s^2\mu + q^2\mu'' = 2qs \cdot \mu', \quad r^2\mu + p^2\mu'' = 2pr \cdot \mu',$$

so schliesst man mit Rücksicht auf die vorstehende Gleichung leicht

$$(ps + qr) \cdot \mu = 2pq \cdot \mu', \quad (ps + qr) \cdot \mu'' = 2rs \cdot \mu',$$

welche Gleichungen, mit der zweiten jener Beziehungen verbunden, sogleich

$$\mu' = \varepsilon \cdot (ps + qr), \quad \mu = \varepsilon \cdot 2pq, \quad \mu'' = \varepsilon \cdot 2rs$$

liefern, wo unter ε eine Einheit verstanden ist; diese aber ergiebt sich als $+1$, wenn man verlangt, was geschehen soll, dass die Transformation (47) eine positive ist.

Hiernach findet man alle positive Transformationen der Form $zz'' - z'^2$ in sich selbst mittels des Schemas:

$$(48) \qquad \begin{cases} z = p^2 \cdot \zeta + 2pq \cdot \zeta' + q^2 \cdot \zeta'' \\ z' = pr \cdot \zeta + (ps + qr) \cdot \zeta' + qs \cdot \zeta'' \\ z'' = r^2 \cdot \zeta + 2rs \cdot \zeta' + s^2 \cdot \zeta'' \end{cases}$$

wenn man für p, q, r, s alle Werthe setzt, welche die Bedingung

$$(49) \qquad ps - qr = 1$$

erfüllen.

8. Nunmehr hat es theoretisch keine Schwierigkeit, durch Anwendung des in nr. 5 ausgesprochenen Satzes alle positiven Transformationen einer beliebigen ternären quadratischen Form in sich selbst zu finden. Man nehme nach nr. 6 eine beliebige Substitution (37) — wir nennen sie T — welche f in

$$4D(zz'' - z'^2)$$

verwandelt, setze sie zusammen mit einer Substitution (48), welche Σ heisse, und setze endlich die resultirende Substitution zusammen mit T' d. h. mit der Umkehrung von T, so erhält man eine der gesuchten Transformationen mit positivem Modulus, und man erhält diese alle, wenn man für Σ die sämmtlichen durch das Schema (48) gelieferten Sub-

stitutionen der Reihe nach wählt, ausgedrückt, wie es der Fall sein muss, mit Hilfe dreier willkürlich bleibender Grössen oder vielmehr mittels der vier durch die Bedingungsgleichung (49) unter einander verbundenen Grössen p, q, r, s.

Führt man statt der letztern durch die Gleichungen

$$(50)\qquad \begin{cases} p = t - u\alpha_0' - u'\alpha_1' - u''\alpha_2' \\ q = - u\alpha_0'' - u'\alpha_1'' - u''\alpha_2'' \\ r = \phantom{t - {}} u\alpha_0^0 + u'\alpha_1^0 + u''\alpha_2^0 \\ s = t + u\alpha_0' + u'\alpha_1' + u''\alpha_2' \end{cases}$$

vier andere Grössen t, u, u', u'' ein, welche folglich, ausgedrückt durch jene, folgendermassen bestimmt sind:

$$(51)\qquad \begin{cases} t = \frac{p+s}{2} \\ 2Du = A_0^0 \cdot r - 2A_0' \cdot \frac{p-s}{2} - A_0'' \cdot q \\ 2Du' = A_1^0 \cdot r - 2A_1' \cdot \frac{p-s}{2} - A_1'' \cdot q \\ 2Du'' = A_2^0 \cdot r - 2A_2' \cdot \frac{p-s}{2} - A_2'' \cdot q, \end{cases}$$

so werden t, u, u', u'' der Identität (43) zufolge durch folgende beachtenswerthe Gleichung

$$(52)\qquad t^2 + F(u, u', u'') = 1$$

unter einander verbunden sein. Diese Grössen t, u, u', u'' sind es dann, welche in den Elementen der Transformation der Form $f(x, x', x'')$ in sich selbst ausser den Coefficienten dieser Form allein noch verbleiben; die Elemente der Substitution T fallen, wie es der Natur der Sache entspricht, bei Ausführung der Rechnung aus der Betrachtung vollkommen heraus; indem man jene vier Grössen auf alle mit der Bedingungsgleichung (52) verträgliche Weise wählt, erhält man sämmtliche positive Transformationen der Form $f(x, x', x'')$ in sich selbst.

Aber die wirkliche Herstellung dieser Transformationen durch Ausführung der angedeuteten Rechnung, obwohl sie keinen weiteren Schwierigkeiten begegnet, ist nicht ohne grosse Weitläufigkeit; indem wir daher hier bezüglich dieses Punktes auf Cantors Abhandlung verweisen, ziehen wir vor, nun-

mehr die Transformationen der ternären quadratischen Formen in sich selbst ohne das Hilfsmittel einer Zwischenform aus den, die Transformation charakterisirenden Bedingungsgleichungen unmittelbar herzuleiten.

9. Diese Bedingungsgleichungen ergeben sich aus (27), indem man die Form f_1 mit der Form f identificirt, als die folgenden:

$$(53)\quad \begin{cases} a = f_0^0\cdot\alpha_0^0 + f_0^1\cdot\alpha_1^0 + f_0^2\cdot\alpha_2^0 \\ a' = f_1^0\cdot\alpha_0' + f_1^1\cdot\alpha_1' + f_1^2\cdot\alpha_2' \\ a'' = f_2^0\cdot\alpha_0'' + f_2^1\cdot\alpha_1'' + f_2^2\cdot\alpha_2'' \\ b = f_1^0\cdot\alpha_0''+f_1^1\cdot\alpha_1''+f_1^2\cdot\alpha_2'' = f_2^0\cdot\alpha_0' + f_2^1\cdot\alpha_1' + f_2^2\cdot\alpha_2' \\ b' = f_2^0\cdot\alpha_0^0 + f_2^1\cdot\alpha_1^0 + f_2^2\cdot\alpha_2^0 = f_0^0\cdot\alpha_0'' + f_0^1\cdot\alpha_1'' + f_0^2\cdot\alpha_2'' \\ b'' = f_0^0\cdot\alpha_0' + f_0^1\cdot\alpha_1' + f_0^2\cdot\alpha_2' = f_1^0\cdot\alpha_0^0 + f_1^1\cdot\alpha_1^0 + f_1^2\cdot\alpha_2^0. \end{cases}$$

Wird aber f_1 identisch mit f, so wird es auch die Adjungirte F_1 mit F, und den in nr. 4 abgeleiteten allgemeinen Beziehungen zufolge wird die Substitution (32) eine positive Transformation von F in sich selbst darstellen, wenn (24) eine solche Transformation von f in sich selbst ist. Man erhält demnach neben den Gleichungen (53) auch die folgenden:

$$(54)\quad \begin{cases} A = F_0^0\cdot\alpha_0^0 + F_0^1\cdot\alpha_0' + F_0^2\cdot\alpha_0'' \\ A' = F_1^0\cdot\alpha_1^0 + F_1^1\cdot\alpha_1' + F_1^2\cdot\alpha_1'' \\ A'' = F_2^0\cdot\alpha_2^0 + F_2^1\cdot\alpha_2' + F_2^2\cdot\alpha_2'' \\ B = F_1^0\cdot\alpha_2^0 + F_1^1\cdot\alpha_2' + F_1^2\cdot\alpha_2'' \\ \quad = F_2^0\cdot\alpha_1^0 + F_2^1\cdot\alpha_1' + F_2^2\cdot\alpha_1'' \\ B' = F_2^0\cdot\alpha_0^0 + F_2^1\cdot\alpha_0' + F_2^2\cdot\alpha_0'' \\ \quad = F_0^0\cdot\alpha_2^0 + F_0^1\cdot\alpha_2' + F_0^2\cdot\alpha_2'' \\ B'' = F_0^0\cdot\alpha_1^0 + F_0^1\cdot\alpha_1' + F_0^2\cdot\alpha_1'' \\ \quad = F_1^0\cdot\alpha_0^0 + F_1^1\cdot\alpha_0' + F_1^2\cdot\alpha_0'', \end{cases}$$

wenn zur Abkürzung

$$(55)\quad \begin{cases} F(\alpha_i^0, \alpha_i', \alpha_i'') = F_i \\ \frac{1}{2}\frac{\partial F_i}{\partial \alpha_i^k} = F_i^k \end{cases}$$

gesetzt wird.

Aus diesen durch die Aufgabe selbst gegebenen Beziehungen folgert man nun vor allem eine charakteristische Eigenschaft jeder Transformation einer ternären quadratischen Form in sich selbst, eine Eigenschaft, welche unabhängig ist von der besonderen Form, die jene in sich selbst verwandelt. Zunächst ergeben die Gleichungen (54) diese andern:

$$(56)\quad \begin{cases} A \cdot \mathsf{A}_0^k + B'' \cdot \mathsf{A}_1^k + B' \cdot \mathsf{A}_2^k = \frac{1}{2}\frac{\partial F_0}{\partial \alpha_0^k} \\ B'' \cdot \mathsf{A}_0^k + A' \cdot \mathsf{A}_1^k + B \cdot \mathsf{A}_2^k = \frac{1}{2}\frac{\partial F_1}{\partial \alpha_1^k} \\ B' \cdot \mathsf{A}_0^k + B \cdot \mathsf{A}_1^k + A'' \cdot \mathsf{A}_2^k = \frac{1}{2}\frac{\partial F_2}{\partial \alpha_2^k} \end{cases}$$

und aus ihnen folgt, wenn sie, je nachdem $k = 0, 1, 2$ ist, mit a, b'', b', mit b'', a', b, mit b', b, a'' multiplicirt und addirt, darauf auch die so entstehenden drei Gleichungen addirt werden, folgende merkwürdige Beziehung:

$$(57)\qquad \mathsf{A}_0^0 + \mathsf{A}_1^1 + \mathsf{A}_2^2 = \alpha_0^0 + \alpha_1' + \alpha_2''.$$

Denkt man sich neben der Substitution (24) die Gleichung

$$(58)\qquad \begin{vmatrix} \alpha_0^0 - s, & \alpha_0', & \alpha_0'' \\ \alpha_1^0, & \alpha_1' - s, & \alpha_1'' \\ \alpha_2^0, & \alpha_2', & \alpha_2'' - s \end{vmatrix} = 0,$$

welche die zur Substitution (24) gehörige *Fundamentalgleichung* heissen soll, und, entwickelt, auch so geschrieben werden kann:

$$(58\text{a})\quad -s^3 + (\alpha_0^0 + \alpha_1' + \alpha_2'')s^2 - (\mathsf{A}_0^0 + \mathsf{A}_1' + \mathsf{A}_2'')s + 1 = 0,$$

so ergiebt sich aus (57) ohne weiteres der eigenthümliche Satz: Für jede Transformation einer ternären quadratischen Form in sich selbst ist die zugehörige Fundamentalgleichung eine reciproke Gleichung.

Um aber die gestellte Aufgabe zu lösen, bemerke man zuvörderst die mittels der Beziehungen (6) und (54) nachweisbaren Formeln:

$$f_0^i \cdot F_i^0 + f_1^i \cdot F_i^1 + f_2^i \cdot F_i^2 = D$$

$$f_i^0 \cdot F_i^0 + f_i^1 \cdot F_i^1 + f_i^2 \cdot F_i^2 = D(\alpha_0^i \alpha_i^0 + \alpha_1^i \alpha_i' + \alpha_2^i \alpha_i''),$$

durch deren Subtraktion sich ferner

$$(f_i^0 - f_0^i) \cdot F_i^0 + (f_i^1 - f_1^i) F_i^1 + (f_i^2 - f_2^i) F_i^2$$
$$= D(\alpha_0^i \alpha_i^0 + \alpha_1^i \alpha_i' + \alpha_2^i \alpha_i'' - 1)$$

ergiebt. Denkt man diese letzte Formel für $i = 0, 1, 2$ gebildet, so erhält man durch Addition der entsprechenden Gleichungen eine andere, deren linke Seite der Ausdruck

$$(F_2^1 - F_1^2)(f_2^1 - f_1^2) + (F_0^2 - F_2^0)(f_0^2 - f_2^0)$$
$$+ (F_1^0 - F_0^1)(f_1^0 - f_0^1),$$

deren rechte Seite aber gleich

$$D((\alpha_0^0 + \alpha_1' + \alpha_2'')^2 - 2(\mathsf{A}_0^0 + \mathsf{A}_1' + \mathsf{A}_2'') - 3)$$

ist, also mit Rücksicht auf (57) einfacher

$$D((\alpha_0^0 + \alpha_1' + \alpha_2'' - 1)^2 - 4)$$

geschrieben werden kann. Setzt man demnach

(59) $F_2^1 - F_1^2 = 2Du,\ F_0^2 - F_2^0 = 2Du',\ F_1^0 - F_0^1 = 2Du''$,

woraus, wie leicht einzusehen,

$$(60)\qquad \begin{cases} 2(Au + B''u' + B'u'') = f_1^2 - f_2^1 \\ 2(B''u + A'u' + Bu'') = f_2^0 - f_0^2 \\ 2(B'u + Bu' + A''u'') = f_0^1 - f_1^0 \end{cases}$$

hervorgeht, und setzt man ferner

(61) $\alpha_0^0 + \alpha_1' + \alpha_2'' - 1 = \mathsf{A}_0^0 + \mathsf{A}_1' + \mathsf{A}_2'' - 1 = 2t$,

so findet man sogleich zwischen den Grössen t, u, u', u'' nachstehende Beziehung:

$$(62)\qquad t^2 + F(u, u', u'') = 1$$

und somit den Satz: Jede (positive) Transformation der Form $f(x, x', x'')$ in sich selbst liefert vermittelst der Formeln (59) und (61) eine bestimmte Auflösung der Gleichung (62).

10. Nehmen wir nun zuerst an, für die Transformation (24) finde die Gleichung

$$0 = \alpha_0^0 + \alpha_1' + \alpha_2'' + 1 = \mathsf{A}_0^0 + \mathsf{A}_1' + \mathsf{A}_2'' + 1 = 2(t + 1)$$

nicht statt, was man auch so ausdrücken kann: die zur Transformation gehörige Fundamentalgleichung habe nicht die Wurzel -1, und versuchen, die Transformation durch die Grössen t, u, u', u'' auszudrücken. Zu diesem Zwecke bedienen

wir uns der Gleichungen (56) und (59). Nach ihnen darf man schreiben:

$$
\begin{aligned}
A(\mathsf{A}_0''-\alpha_2^0)+B''(\mathsf{A}_1''-\alpha_2')+B'(\mathsf{A}_2''-\alpha_2'')&=2Du'\\
B''(\mathsf{A}_0''-\alpha_2^0)+A'(\mathsf{A}_1''-\alpha_2')+B(\mathsf{A}_2''-\alpha_2'')&=-2Du\\
B'(\mathsf{A}_0''-\alpha_2^0)+B(\mathsf{A}_1''-\alpha_2')+A''(\mathsf{A}_2''-\alpha_2'')&=0.
\end{aligned}
$$

Indem wir letztere Gleichungen mit a, b'', b' multipliciren und dann addiren, schliessen wir die erste, und auf ähnliche Weise die übrigen der nachstehenden Gleichungen:

$$
(63)\quad \mathsf{A}_0''-\alpha_2^0=2(au'-b''u),\quad \mathsf{A}_1''-\alpha_2'=2(b''u'-a'u),\quad \mathsf{A}_2''-\alpha_2''=2(b'u'-bu),
$$

welche, einmal mit x, x', x'', das andere Mal mit y, y', y'' multiplicirt und jedesmal addirt, im Hinblick auf die zwischen den x und den y angenommenen Beziehungen (24) und (29) die folgenden:

$$
\begin{aligned}
y''-(\alpha_2^0x+\alpha_2'x'+\alpha_2''x'')&=2(u'f^0(x)-uf^1(x))\\
\mathsf{A}_0''y+\mathsf{A}_1''y'+\mathsf{A}_2''y''-x''&=2(u'f^0(y)-uf^1(y))
\end{aligned}
$$

und endlich durch deren Addition die letzte Gleichung des nachstehenden Schemas liefern, von denen die übrigen auf entsprechendem Wege gefunden werden:

$$
(64)\quad \left\{
\begin{aligned}
&(t+1)y-u''f^1(y)+u'f^2(y)\\
=&(t+1)x+u''f^1(x)-u'f^2(x)\\
&(t+1)y'-uf^2(y)+u''f^0(y)\\
=&(t+1)x'+uf^2(x)-u''f^0(x)\\
&(t+1)y''-u'f^0(y)+uf^1(y)\\
=&(t+1)x''+u'f^0(x)-uf^1(x).
\end{aligned}
\right.
$$

Nun kann man statt der Grössen t, u, u', u'' durch die folgenden Gleichungen:

$$
(65)\quad t+1=2p^2,\quad u=2pq,\quad u'=2pq',\quad u''=2pq'',
$$

wenn man p positiv vorschreibt, auf eindeutige Weise vier andere Grössen p, q, q', q'' einführen, welche wegen der Bedingung (62) durch die Gleichung

$$
(66)\qquad p^2+F(q,q',q'')=1
$$

mit einander verbunden sind, und dadurch nehmen die ge-

fundenen Formeln folgende Gestalt an:

$$(67)\quad \begin{cases} p(x-y) = q'(f^2(x)+f^2(y)) - q''(f^1(x)+f^1(y)) \\ p(x'-y') = q''(f^0(x)+f^0(y)) - q(f^2(x)+f^2(y)) \\ p(x''-y'') = q(f^1(x)+f^1(y)) - q'(f^0(x)+f^0(y)). \end{cases}$$

Diese Gleichungen sind die gewünschte Darstellung der Transformation in unentwickelter Gestalt. Um sie in entwickelter Form zu finden, sei zuerst die beachtenswerthe Folgerung hervorgehoben, zu der jene Formeln unmittelbar führen und welche in der Gleichung

$$(68)\qquad qx + q'x' + q''x'' = qy + q'y' + q''y''$$

ihren Ausdruck findet. Wenn man sie ferner mit a, b'', b', ein andermal mit b'', a', b, ein drittes Mal mit b', b, a'' multiplicirt und jedesmal addirt, findet man aus ihnen noch diese Beziehungen:

$$(69)\quad \begin{cases} p(f^0(x)-f^0(y)) = F^1(q)\cdot(x''+y'') - F^2(q)\cdot(x'+y') \\ p(f^1(x)-f^1(y)) = F^2(q)\cdot(x+y) - F^0(q)\cdot(x''+y'') \\ p(f^2(x)-f^2(y)) = F^0(q)\cdot(x'+y') - F^1(q)\cdot(x+y); \end{cases}$$

werden aber darauf den letztern die Werthe von $f^0(x)$, $f^1(x)$, $f^2(x)$ entnommen, um sie in die Gleichungen (67) einzusetzen, so ergiebt sich, mit alleiniger Beachtung von (66) und (68), das folgende System von Gleichungen:

$$(70)\quad \begin{cases} x = (2p^2-1)y - 2p(q''f^1(y) - q'f^2(y)) \\ \qquad\qquad + 2F^0(q)\cdot(qy+q'y'+q''y'') \\ x' = (2p^2-1)y' - 2p(qf^2(y) - q''f^0(y)) \\ \qquad\qquad + 2F^1(q)\cdot(qy+q'y'+q''y'') \\ x'' = (2p^2-1)y'' - 2p(q'f^0(y) - qf^1(y)) \\ \qquad\qquad + 2F^2(q)\cdot(qy+q'y'+q''y''). \end{cases}$$

Diese neuen Formeln stellen also die Transformation dar, ausgedrückt vermittelst der zugehörigen Lösung t, u, u', u'' der Gleichung (62) oder der vier ihr entsprechenden Grössen p, q, q', q''.

Aber es bilden auch für jede Lösung der Gleichung (62), bei welcher $t+1$ von Null verschieden ist, die Gleichungen (64) in unentwickelter, die Gleichungen (70) in entwickelter Gestalt eine positive

Transformation der Form $f(x, x', x'')$ in sich selbst von der eben betrachteten Art. Denn

Erstens haben die in x, x', x'' resp. in y, y', y'' linearen Ausdrücke zur Rechten und Linken der Gleichungen (64) dann dieselbe von Null verschiedene Determinante, nämlich $2(t+1)^2$, und folglich müssen die Gleichungen, wenn sie nach x, x', x'' aufgelöst werden, die Determinante $+1$ haben.

Zweitens findet sich, wenn jene Gleichungen mit

$$f^0(x) + f^0(y), \quad f^1(x) + f^1(y), \quad f^2(x) + f^2(y)$$

multiplicirt und dann addirt werden, ohne weiteres die Gleichheit

$$(t+1) \cdot f(y, y', y'') = (t+1) \cdot f(x, x', x'')$$

d. i.

$$f(y, y', y'') = f(x, x', x'').$$

Drittens ist die Summe aus dem Coefficienten von y in der ersten, von y' in der zweiten und von y'' in der dritten Gleichung (70) vermehrt um die Einheit gleich $2(t+1)$ also von Null verschieden.

Und somit lässt sich folgendes Resultat aussprechen: Die Formeln (70) liefern alle positiven Transformationen der Form $f(x, x', x'')$ in sich selbst, bei denen die Gleichung

$$\alpha_0^0 + \alpha_1' + \alpha_2'' + 1 = A_0^0 + A_1' + A_2'' + 1 = 0$$

nicht stattfindet, und jede ein Mal, wenn darin für p, q, q', q'' alle möglichen der Gleichung (66) genügenden Werthsysteme gesetzt werden, deren p positiv ist.

11. Nunmehr betrachten wir diejenigen (positiven) Transformationen, für welche

$$(71) \qquad \alpha_0^0 + \alpha_1' + \alpha_2'' + 1 = A_0^0 + A_1' + A_2'' + 1 = 0$$

ist, und wollen zeigen, dass auch sie sämmtlich aus den Formeln (70) erhalten werden, wenn man darin für p, q, q', q'' diejenigen Lösungen der Gleichung (66) einsetzt, bei welchen $p = 0$, q, q', q'' also Zahlen sind, welche die Bedingung erfüllen:

$$(72) \qquad F(q, q', q'') = 1.$$

Denn erstens erhält man auf solche Weise die Substitution

$$(73)\qquad \begin{cases} x = -y + 2F^0(q)\cdot(qy + q'y' + q''y'') \\ x' = -y' + 2F^1(q)\cdot(qy + q'y' + q''y'') \\ x'' = -y'' + 2F^2(q)\cdot(qy + q'y' + q''y''), \end{cases}$$

von der man sich leicht überzeugt, dass sie die Gleichung

$$f(x, x', x'') = f(y, y', y'')$$

befriedigt, während ihre Determinante gleich

$$-1 + 2F(q, q', q'') = +1$$

und die Summe aus dem ersten, fünften und letzten Substitutionscoefficienten gleich

$$-3 + 2F(q, q', q'') = -1$$

gefunden wird.

Zweitens sei die Transformation (24) eine der jetzt betrachteten, also $t + 1 = 0$, so lässt sich zunächst beweisen, dass die zugehörigen Grössen u, u', u'' gleich Null sein müssen. Denn alsdann führen die Gleichungen (63), wenn sie mit $\alpha_0'', \alpha_1'', \alpha_2''$ multiplicirt und dann addirt werden, wegen (71) zu der folgenden:

$$\alpha_2'' - A_2'' = 2(u'f_2^0 - uf_2^1)$$

und geben, mit der letzten jener Gleichungen verglichen, die Beziehung

$$u'(b' + f_2^0) = u(b + f_2^1),$$

zu welcher auf ganz entsprechende Weise noch folgende andere hinzukommen:

$$\begin{aligned} u'(b'' + f_1^0) &= u(a' + f_1^1) \\ u'(a + f_0^0) &= u(b'' + f_0^1) \\ u''(b + f_2^1) &= u'(a'' + f_2^2) \\ u''(a' + f_1^1) &= u'(b + f_1^2) \\ u''(b'' + f_0^1) &= u'(b' + f_0^2) \\ u(a'' + f_2^2) &= u''(b' + f_2^0) \\ u(b + f_1^2) &= u''(b'' + f_1^0) \\ u(b' + f_0^2) &= u''(a + f_0^0). \end{aligned}$$

Ihnen zufolge dürfte man nun, wenn u, u', u'' nicht sämmtlich gleich Null wären,

$$a + f_0^0 = 2Duz,\quad b'' + f_0^1 = 2Du'z,\quad b' + f_0^2 = 2Du''z$$
$$b'' + f_1^0 = 2Duz',\quad a' + f_1^1 = 2Du'z',\quad b + f_1^2 = 2Du''z'$$
$$b' + f_2^0 = 2Duz'',\quad b + f_2^1 = 2Du'z'',\quad a'' + f_2^2 = 2Du''z''$$

setzen. Aus diesen Gleichungen folgt aber einerseits ohne Mühe das folgende System:

$$\alpha_0^0 = -1 + z\frac{\partial F}{\partial u},\quad \alpha_0' = z'\frac{\partial F}{\partial u},\quad \alpha_0'' = z''\frac{\partial F}{\partial u}$$
$$\alpha_1^0 = z\frac{\partial F}{\partial u'},\quad \alpha_1' = -1 + z'\frac{\partial F}{\partial u'},\quad \alpha_1'' = z''\frac{\partial F}{\partial u'}$$
$$\alpha_2^0 = z\frac{\partial F}{\partial u''},\quad \alpha_2' = z'\frac{\partial F}{\partial u''},\quad \alpha_2'' = -1 + z''\frac{\partial F}{\partial u''}$$

mit der Determinante

$$-1 + z\frac{\partial F}{\partial u} + z'\frac{\partial F}{\partial u'} + z''\frac{\partial F}{\partial u''}.$$

Andererseits ergeben sie

$$2D(z'u'' - z''u') = f_1^2 - f_2^1 = \frac{\partial F}{\partial u}$$
$$2D(z''u - zu'') = f_2^0 - f_0^2 = \frac{\partial F}{\partial u'}$$
$$2D(zu' - z'u) = f_0^1 - f_1^0 = \frac{\partial F}{\partial u''}$$

und nach der zweiten Grundformel ist

$$4 \cdot F(z, z', z'') \cdot F(u, u', u'') = \left(z\frac{\partial F}{\partial u} + z'\frac{\partial F}{\partial u'} + z''\frac{\partial F}{\partial u''}\right)^2$$
$$+ 4 \cdot D \cdot f(z'u'' - z''u', z''u - zu'', zu' - z'u)$$

d. i. mit Rücksicht auf die voraufgehenden Formeln und auf die Beziehungen in nr. 1 gleich

$$\left(z\frac{\partial F}{\partial u} + z'\frac{\partial F}{\partial u'} + z''\frac{\partial F}{\partial u''}\right)^2 + 4F(u, u', u'').$$

Da aber für die jetzt betrachteten Transformationen

$$F(u, u', u'') = 0$$

ist, findet sich

$$z\frac{\partial F}{\partial u} + z'\frac{\partial F}{\partial u'} + z''\frac{\partial F}{\partial u''} = 0$$

also die obige Determinante gleich -1, nicht $+1$, wie es von der Transformation vorausgesetzt ist. —

Da hiernach u, u', u'' sämmtlich gleich Null sein müssen, finden nach (59) die Gleichungen statt:

$$F_2^1 = F_1^2, \quad F_0^2 = F_2^0, \quad F_1^0 = F_0^1,$$

durch welche leicht die folgenden sich bestätigen lassen:

$$\begin{aligned}
(a\ + f_0^0)(a' + f_1') &= (b'' + f_1^0)(b'' + f_0^1)\\
(a' + f_1')(a'' + f_2'') &= (b\ + f_2^1)(b\ + f_1^2)\\
(a'' + f_2'')(a\ + f_0^0) &= (b' + f_0^2)(b' + f_2^0)\\
(a\ + f_0^0)(b\ + f_1^2) &= (b' + f_0^2)(b'' + f_1^0)\\
(a' + f_1^1)(b' + f_2^0) &= (b'' + f_1^0)(b\ + f_2^1)\\
(a'' + f_2^2)(b'' + f_0^1) &= (b\ + f_2^1)(b' + f_0^2).
\end{aligned}$$

Ihnen gemäss darf man setzen

$$\begin{array}{lll}
a\ + f_0^0 = 2Dq^2, & b'' + f_0^1 = 2Dqq', & b' + f_0^2 = 2Dqq''\\
b'' + f_1^0 = 2Dq'q, & a' + f_1^1 = 2Dq'^2, & b\ + f_1^2 = 2Dq'q''\\
b' + f_2^0 = 2Dq''q, & b\ + f_2^1 = 2Dq''q', & a'' + f_2^2 = 2Dq''^2
\end{array}$$

und erschliesst hieraus das System:

$$\begin{array}{lll}
\alpha_0^0 = -1 + q\dfrac{\partial F}{\partial q}, & \alpha_0' = q'\dfrac{\partial F}{\partial q}, & \alpha_0'' = q''\dfrac{\partial F}{\partial q}\\
\alpha_1^0 = q\dfrac{\partial F}{\partial q'}, & \alpha_1' = -1 + q'\dfrac{\partial F}{\partial q'}, & \alpha_1'' = q''\dfrac{\partial F}{\partial q'}\\
\alpha_2^0 = q\dfrac{\partial F}{\partial q''}, & \alpha_2' = q'\dfrac{\partial F}{\partial q''}, & \alpha_2'' = -1 + q''\dfrac{\partial F}{\partial q''}
\end{array}$$

mit der Determinante

$$-1 + 2 \cdot F(q, q', q'');$$

also muss, da letztere $+1$ sein soll, die Gleichung (72) erfüllt sein. Die betrachtete Substitution ist mithin eine von denen, welche in (73) verzeichnet sind.

Uebrigens ist ersichtlich, dass die Werthsysteme q, q', q'' und $-q, -q', -q''$ dieselbe Transformation liefern also nur eins von ihnen beizubehalten ist.

Da hiermit der gewollte Nachweis geliefert ist, so ersieht man schliesslich, dass die Formeln (70) oder, anders geordnet, die folgenden Substitutionen:

$$(70a)\quad \left\{\begin{array}{l}
2p^2-1+2pq'b'-2pq''b''+2qF^0(q),\\
2pq'b-2pq''a'+2q'F^0(q),\\
2pq'a''-2pq''b+2q''F^0(q);\\
2pq''a-2pqb'+2qF^1(q),\\
2p^2-1+2pq''b''-2pqb+2q'F^1(q),\\
2pq''b'-2pqa''+2q''F^1(q);\\
2pqb''-2pq'a+2qF^2(q),\\
2pqa'-2pq'b''+2q'F^2(q),\\
2p^2-1+2pqb-2pq'b'+2q''F^2(q)
\end{array}\right\}$$

der allgemeine Ausdruck *aller positiven Transformationen der Form* $f(x, x', x'')$ *in sich selbst* sind.

12. Hier seien an diese Formeln noch einige wenige Bemerkungen angeschlossen.

Zunächst kann man ihnen eine zweite, wesentlich abweichende Form geben mittels folgender Ueberlegung. Bedeutet die Substitution (24) eine Transformation der Form $f(x, x', x'')$ in sich selbst, so lehren die Sätze der nr. 4, da in diesem Falle f_1 mit f also auch F_1 mit F identisch wird, dass die Adjungirte $F(X, X', X'')$ durch die transponirte Substitution in sich selbst übergeht, sowie auch umgekehrt. Stellt man hiernach in Analogie mit (70) die Formeln auf, welche die Form F in sich selbst transformiren, wobei zu beachten ist, dass die Adjungirte von F mit $D \cdot f$ identisch ist, und transponirt dann die Substitution, so muss man die Transformationen von f in sich selbst erhalten. So gewinnt man für dieselben die folgende zweite Gestalt:

$$(70b)\quad \left\{\begin{array}{l}
2p^2-1+2pq'B'-2pq''B''+2qDf^0(q),\\
2pq''A-2pqB'+2qDf^1(q),\\
2pqB''-2pq'A+2qDf^2(q);\\
2pq'B-2pq''A'+2q'Df^0(q),\\
2p^2-1+2pq''B''-2pqB+2q'Df^1(q),\\
2pqA'-2pq'B''+2q'Df^2(q);\\
2pq'A''-2pq''B+2q''Df^0(q),\\
2pq''B'-2pqA''+2q''Df^1(q),\\
2p^2-1+2pqB-2pq'B'+2q''Df^2(q)
\end{array}\right\}$$

wobei die Grössen p, q, q', q'' jetzt durch die Gleichung

$$(74) \qquad p^2 + D \cdot f(q, q', q'') = 1$$

mit einander verbunden zu denken sind.

Die Gleichungen (67), welche die Transformation (70) in unentwickelter Gestalt geben, haben das Eigenthümliche, dass sie sowohl diese Transformation selbst — die aus ihnen erhalten wird, wenn man sie nach x, x', x'' auflöst — als auch die umgekehrte Transformation enthalten, die man aus ihnen findet, löst man sie auf nach y, y', y''. Aber jene Gleichungen bleiben ungeändert, wenn man bei Vertauschung von $x, x' x''$ mit y, y', y'' gleichzeitig q, q', q'' mit entgegengesetzten Vorzeichen nimmt. Hieraus ist klar, dass man aus den Formeln (70) die inverse Substitution auf dieselbe Weise d. h. — abgesehen von der Bezeichnung der Veränderlichen — einfach durch Vertauschung von q, q', q'' mit $-q, -q', -q''$ erhält.

Endlich soll untersucht werden, wie sich die Transformation schreiben lässt, welche aus zwei der Transformationen (70) zusammengesetzt ist*). Die Formeln (70) gingen unmittelbar aus den Gleichungen (67) hervor, die man auch rückwärts wieder aus ihnen erhalten kann, wenn p von Null verschieden; aber auch die speciellen Transformationen (73), welche $p = 0$ entsprechen, führen, wie unmittelbar zu sehen, zu den Gleichungen

$$f^0(x) = -f^0(y) + 2Dq(qy + q'y' + q''y'')$$
$$f^1(x) = -f^1(y) + 2Dq'(qy + q'y' + q''y'')$$
$$f^2(x) = -f^2(y) + 2Dq''(qy + q'y' + q''y'')$$

und demnach zu den folgenden

$$0 = q'(f^2(x) + f^2(y)) - q''(f^1(x) + f^1(y))$$
$$0 = q''(f^0(x) + f^0(y)) - q(f^2(x) + f^2(y))$$
$$0 = q(f^1(x) + f^1(y)) - q'(f^0(x) + f^0(y))$$

d. i. zu den Gleichungen (67) für $p = 0$. Man darf also, statt

*) Vgl. hierzu in Darboux' Bull. des Sciences mathématiques XI den Aufsatz von Tannery, sur les substitutions linéaires par lesquelles une forme quadratique ternaire se reproduit elle-même, p. 229; auch G. Cantor de transform. formar. ternar. quadrat. S. 10.

mit den Gleichungen (70), mit den Gleichungen (67) operiren. Nenne man mithin T die durch sie ausgedrückte Transformation und betrachte eine zweite Transformation T^1, welche durch die analogen Formeln

$$
(75) \quad \begin{cases} r(y-z) = s'(f^2(z)+f^2(y)) - s''(f^1(z)+f^1(y)) \\ r(y'-z') = s''(f^0(z)+f^0(y)) - s(f^2(z)+f^2(y)) \\ r(y''-z'') = s(f^1(z)+f^1(y)) - s'(f^0(z)+f^0(y)) \end{cases}
$$

ausgedrückt ist und welcher die folgenden mit (69) analogen Formeln zugehören:

$$
(76) \quad \begin{cases} r(f^0(y)-f^0(z)) = F^1(s)\cdot(y''+z'') - F^2(s)\cdot(y'+z') \\ r(f^1(y)-f^1(z)) = F^2(s)\cdot(y+z) - F^0(s)\cdot(y''+z'') \\ r(f^2(y)-f^2(z)) = F^0(s)\cdot(y'+z') - F^1(s)\cdot(y+z). \end{cases}
$$

Man wird die zusammengesetzte Transformation $T \cdot T^1$ erhalten, wenn man zwischen den Gleichungen (67) und (75) die Veränderlichen y, y', y'' eliminirt. Entnimmt man zu diesem Zwecke aus den letztgeschriebenen Gleichungen $f^1(y)$, $f^2(y)$, um sie in die erste der Gleichungen (67) einzusetzen, so findet man zunächst

$$
\begin{aligned} pr(x-y) = {} & q'r(f^2(x)+f^2(z)) - q''r(f^1(x)+f^1(z)) \\ & + F^0(s)[q(y+z)+q'(y'+z')+q''(y''+z'')] \\ & - (y+z)(qF^0(s)+q'F^1(s)+q''F^2(s)). \end{aligned}
$$

Entnimmt man dagegen aus den Gleichungen (69) die Werthe von $f^1(y)$, $f^2(y)$, um sie in die erste der Gleichungen (75) einzusetzen, so findet man gleicherweise

$$
\begin{aligned} pr\cdot(y-z) = {} & ps'(f^2(x)+f^2(z)) - ps''(f^1(x)+f^1(z)) \\ & - F^0(q)[s(x+y)+s'(x'+y')+s''(x''+y'')] \\ & + (x+y)(sF^0(q)+s'F^1(q)+s''F^2(q)). \end{aligned}
$$

Diese Gleichung addire man nun zur vorigen, bemerke aber dabei, dass nach (68)

$$qy + q'y' + q''y'' = qx + q'x' + q''x''$$

und ebenso

$$sy + s'y' + s''y'' = sz + s'z' + s''z'',$$

sowie dass

$$s\cdot F^0(q) + s'\cdot F^1(q) + s''\cdot F^2(q) = q\cdot F^0(s) + q'\cdot F^1(s) + q''\cdot F^2(s)$$

ist. So erhält man dann

$$(pr - qF^0(s) - q'F^1(s) - q''F^2(s)) \cdot (x - z)$$
$$= (rq' + ps')(f^2(x) + f^2(z)) - (rq'' + ps'')(f^1(x) + f^1(z))$$
$$+ (qF^0(s) - sF^0(q))(x + z) + (q'F^0(s) - s'F^0(q))(x' + z')$$
$$+ (q''F^0(s) - s''F^0(q))(x'' + z'').$$

Da sich aber leicht

$$\begin{aligned} qF^0(s) - sF^0(q) &= b' \cdot \frac{1}{2} \frac{\partial f}{\partial(q''s - qs'')} - b'' \cdot \frac{1}{2} \frac{\partial f}{\partial(qs' - q's)} \\ q'F^0(s) - s'F^0(q) &= b \cdot \frac{1}{2} \frac{\partial f}{\partial(q''s - qs'')} - a' \cdot \frac{1}{2} \frac{\partial f}{\partial(qs' - q's)} \\ q''F^0(s) - s''F^0(q) &= a'' \cdot \frac{1}{2} \frac{\partial f}{\partial(q''s - qs'')} - b \cdot \frac{1}{2} \frac{\partial f}{\partial(qs' - q's)} \end{aligned}$$

ergiebt, wo bei den partiellen Ableitungen kurz f statt

$$f(q's'' - q''s', q''s - qs'', qs' - q's)$$

steht, so lässt sich die vorige Formel einfacher so schreiben:

$$(pr - qF^0(s) - q'F^1(s) - q''F^2(s)) \cdot (x - z)$$
$$= \left(rq' + ps' + \frac{1}{2} \frac{\partial f}{\partial(q''s - qs'')}\right) \cdot (f^2(x) + f^2(z))$$
$$- \left(rq'' + ps'' + \frac{1}{2} \frac{\partial f}{\partial(qs' - q's)}\right) \cdot (f^1(x) + f^1(z)).$$

Man gewinnt also schliesslich die erste der folgenden Gleichungen:

$$(77) \quad \begin{cases} t(x - z) = u'(f^2(x) + f^2(z)) - u''(f^1(x) + f^1(z)) \\ t(x' - z') = u''(f^0(x) + f^0(z)) - u(f^2(x) + f^2(z)) \\ t(x'' - z'') = u(f^1(x) + f^1(z)) - u'(f^0(x) + f^0(z)), \end{cases}$$

von denen die übrigen auf ganz analoge Weise gefunden werden, wenn man zur Abkürzung

$$(78) \quad \begin{cases} pr - qF^0(s) - q'F^1(s) - q''F^2(s) = t \\ qr + ps + \frac{1}{2} \frac{\partial f}{\partial(q's'' - q''s')} = u \\ q'r + p's + \frac{1}{2} \frac{\partial f}{\partial(q''s - qs'')} = u' \\ q''r + p''s + \frac{1}{2} \frac{\partial f}{\partial(qs' - q's)} = u'' \end{cases}$$

setzt. Die Vergleichung dieser Formeln mit den Formeln (21)

zeigt, dass t, u, u', u'' diejenigen Werthe sind, welche aus der Zusammensetzung der Formeln

$$p^2 + F(q, q', q'') \quad \text{und} \quad r^2 + F(s, s', s'')$$

zur Form

$$t^2 + F(u, u', u'')$$

entstehen. Demnach leisten t, u, u', u'' der Gleichung

$$t^2 + F(u, u', u'') = 1$$

Genüge und die Ausdrücke (77) lehren den Satz:

Sind T, T_1 zwei Transformationen (70), welche den Lösungen

$$p, q, q', q''; \quad p_1, q_1, q_1', q_1''$$

der Gleichung (66) entsprechen, so entspricht die aus ihnen zusammengesetzte Transformation $T \cdot T_1$ derjenigen Lösung derselben Gleichung, welche nach der in nr. 3 gegebenen Regel aus der Zusammensetzung der beiden Formen

$$p^2 + F(q, q', q''), \quad p_1^2 + F(q_1, q_1', q_1'')$$

entsteht.

Zweites Capitel.

Grundlegende arithmetische Sätze und Begriffe.

1. Indem wir uns nun zur Betrachtung der arithmetischen Eigenschaften der ternären quadratischen Formen wenden, dürfen und werden wir fortan uns ausschliesslich auf die Betrachtung solcher Formen

$$f(x, x', x'') = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx'$$

beschränken, deren Coefficienten a, a', a'', b, b', b'' — die erstern drei sollen Hauptcoefficienten genannt werden — ganze Zahlen sind. Alsdann werden auch ihre Determinante D sowohl, wie auch die Coefficienten der adjungirten Form

$$F(x, x', x'')$$
$$= Ax^2 + A'x'^2 + A''x''^2 + 2Bx'x'' + 2B'x''x + 2B''xx'$$

ganze Zahlen sein. Wir werden ferner in allem Folgenden, wo nicht das Gegentheil gesagt wird, die Determinante als eine ungerade Zahl voraussetzen. Denn in allen wesentlichen Stücken verhalten sich die Formen mit gerader Determinante durchaus wie diejenigen mit ungerader Determinante, nöthigen jedoch in mannigfaltiger Hinsicht zu umständlichen Unterscheidungen und besonderen Betrachtungen, durch welche die Einfachheit der Entwicklungen und ihre Prägnanz erheblich beeinträchtigt wird und die wir in unserer Darstellung vermeiden wollen. An besonders wichtigen Punkten wollen wir unsern Resultaten auch diejenigen an die Seite stellen, zu welchen die Untersuchung im Falle gerader Determinanten führt, und auf die Arbeiten verweisen, in denen sie entwickelt worden sind.

Man darf sich ferner auf die Betrachtung sogenannter primitiver Formen $f(x, x', x'')$ beschränken, bei welchen die Coefficienten a, a', a'', b, b', b'' keinen von 1 verschiedenen gemeinsamen Theiler haben, denn die übrigen, welche daraus abgeleitet werden, indem man sie mit irgend einer ganzen Zahl multiplicirt, haben keine wesentlichen andern Eigenschaften. Die primitiven Formen aber zerfallen hier, wie in der Lehre von den binären quadratischen Formen, noch weiter in die beiden Arten der eigentlich- und der uneigentlich-primitiven. Denn die Coefficienten $a, a', a'', 2b, 2b', 2b''$ werden entweder, wie die Coefficienten a, a', a'', b, b', b'', den grössten gemeinsamen Theiler $\sigma = 1$ haben, nämlich dann, wenn von den Hauptcoefficienten wenigstens einer ungerade ist, oder den grössten gemeinsamen Theiler $\sigma = 2$, wenn die drei Hauptcoefficienten gerade, also dann von den drei Zahlen b, b', b'' wenigstens eine ungerade ist. Die Formen der ersten Art heissen eigentlich-, die der zweiten Art uneigentlich-primitiv. Hier leuchtet der Gleichung

$$D = aa'a'' + 2bb'b'' - ab^2 - a'b'^2 - a''b''^2$$

zufolge unmittelbar ein, dass es für ungerade Determinanten nur eigentlich-primitive Formen giebt.

Während nun bei den primitiven binären quadratischen Formen eine weitere Eintheilung als die in die eigentlich- und

uneigentlich-primitiven nicht erforderlich ist, hat zuerst Eisenstein darauf hingewiesen, dass bei ternären quadratischen Formen (und überhaupt bei denjenigen mit mehr als zwei Veränderlichen) sich dies ganz anders verhält, und hat eine Eintheilung der primitiven Formen jeder der beiden Arten in sogenannte Ordnungen gelehrt*). Der Gesichtspunkt, von dem aus sie vorzunehmen ist, ist der folgende:

Wenngleich die Coefficienten der Form $f(x, x', x'')$ keinen von 1 verschiedenen gemeinsamen Theiler mehr haben, braucht doch deshalb noch nicht dasselbe der Fall zu sein bei ihrer Adjungirten. Nehmen wir also der Allgemeinheit wegen an, die Coefficienten A, A', A'', B, B', B'' von $F(x, x', x'')$ hätten den grössten gemeinsamen Theiler Ω. Um uns hier an die grundlegende Arbeit von Stephen Smith möglichst anzuschliessen**), soll dieser Theiler positiv genommen werden oder negativ, je nachdem es sich um bestimmte oder unbestimmte Formen handelt. Wenn man dann setzt

$$(1)\qquad \begin{cases} A = \Omega \cdot \mathfrak{A}, & A' = \Omega \cdot \mathfrak{A}', \quad A'' = \Omega \cdot \mathfrak{A}'', \\ B = \Omega \cdot \mathfrak{B}, & B' = \Omega \cdot \mathfrak{B}', \quad B'' = \Omega \cdot \mathfrak{B}'', \end{cases}$$

so werden die Zahlen $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}'', \mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ keinen von 1 verschiedenen Theiler mehr haben, die Form

$$(2)\qquad \begin{aligned} \mathfrak{F}(x, x', x'') = \mathfrak{A}x^2 + \mathfrak{A}'x'^2 + \mathfrak{A}''x''^2 \\ + 2\mathfrak{B}x'x'' + 2\mathfrak{B}'x''x + 2\mathfrak{B}''xx', \end{aligned}$$

also primitiv sein und zugleich die Gleichung

$$(3)\qquad F(x, x', x'') = \Omega \cdot \mathfrak{F}(x, x', x'')$$

Bestand haben. Den Gleichungen (14) des 1. Cap. zufolge sind ersichtlich die Zahlen

$$Da, Da', Da'', Db, Db', Db''$$

sämmtlich theilbar durch Ω^2; da aber f als primitive Form vorausgesetzt worden, folgt hieraus sogleich, dass Ω^2 ein qua-

*) S. Eisenstein's Arbeit: Neue Theoreme der höheren Arithmetik in Cr. J. f. d. r. u. a. Math. 35 S. 177.

**) S. Stephen Smith' vortreffliche Abhandlung: On the Orders and Genera of Ternary Quadratic Forms, in Phil. Transactions of the Royal Society of London, 1867.

dratischer Theiler der Determinante D ist. Setzen wir demgemäss

(4) $$D = \Omega^2 \cdot \Delta.$$

Da nur positive und nur solche unbestimmte Formen betrachtet werden, deren Determinante D positiv ist, wird Δ stets positiv sein; positive Formen unterscheiden sich von den hier allein betrachteten unbestimmten also darin, dass für jene die Zahlen Ω, Δ gleiches, für diese verschiedenes Vorzeichen haben.

Zufolge der Gleichung (3) ist aber die Determinante von F, nämlich $D^2 = \Omega^4 \cdot \Delta^2$, gleich Ω^3 mal derjenigen von $\mathfrak{F}$, und somit ist die Determinante der Form $\mathfrak{F}$ gleich

(5) $$\Delta^2 \cdot \Omega.$$

Endlich ist wegen derselben Gleichung die Adjungirte von F, nämlich $D \cdot f = \Omega^2 \Delta \cdot f$, auch gleich Ω^2 mal der Adjungirten von $\mathfrak{F}$, und deshalb wird die Adjungirte von $\mathfrak{F}$ gleich

(6) $$\Delta \cdot f(x, x', x'').$$

Die mit f und $\mathfrak{F}$ bezeichneten beiden primitiven Formen stehen hiernach zugleich mit den beiden Zahlen Ω, Δ in einer eigenthümlichen Reciprocität: während die Determinante der erstern gleich $\Omega^2\Delta$, ist die der zweiten gleich $\Delta^2\Omega$, und während $\Omega\mathfrak{F}$ die Adjungirte von f, so ist Δf die Adjungirte von $\mathfrak{F}$. Diese reciproke Beziehung der Formen zu einander bewegt uns, jede von ihnen als die Reciproke der andern, also $\mathfrak{F}$ als die Reciproke von f zu benennen*). Wie bemerkt, ist diese Form $\mathfrak{F}$ gleichzeitig mit f primitiv; wird die Determinante D, wie es geschehen soll, und damit auch Ω, Δ ungerade vorausgesetzt, so ist nach (5) auch die Determinante von $\mathfrak{F}$ ungerade, $\mathfrak{F}$ also auch, wie f, eine eigentlich-primitive Form.

Die Eintheilung aller primitiven ternären qua-

*) Diese Benennung hat vor den von andern Mathematikern angewandten, wie: primitive Adjungirte (A. Meyer) oder primitive Contravariante (St. Smith) zugleich den Vorzug grösserer Sachlichkeit und Kürze. Uebrigens ist, wenn f eine unbestimmte Form ist, genau genommen nicht f sondern $-f$ die Reciproke von $\mathfrak{F}$.

dratischen Formen der Determinante D in Ordnungen beruht nun auf dem Grundsatze: alle diejenigen in eine Ordnung zusammenzufassen, für welche die mit Ω, Δ bezeichneten Zahlen dieselben Werthe haben. Da Ω^2 ein quadratischer Theiler von D, durch Ω nach der Formel (4) aber auch Δ bestimmt ist, so kann es nur so viel verschiedene Ordnungen geben, als D quadratische Theiler gestattet, die Einheit mitgerechnet. Handelt es sich insbesondere um eigentlich-primitive Formen, so sind auch diese Ordnungen sämmtlich thatsächlich vorhanden, denn jeder so möglichen Combination Ω, Δ entspricht zum mindesten die eine eigentlich-primitive Form

$$x^2 + \Omega x'^2 + \Omega\Delta x''^2.$$

2. In nr. 4 vorigen Capitels sind zwei Formen f und f_1 einander äquivalent genannt worden, wenn die erstere in die zweite mittels einer linearen Substitution

$$(7)\qquad \begin{cases} x = \alpha_0{}^0 y + \alpha_0{}' y' + \alpha_0{}'' y'' \\ x' = \alpha_1{}^0 y + \alpha_1{}' y' + \alpha_1{}'' y'' \\ x'' = \alpha_2{}^0 y + \alpha_2{}' y' + \alpha_2{}'' y'' \end{cases}$$

transformirt wird, deren Modulus $A = 1$ ist; dann geht auch umgekehrt f_1 durch eine ebensolche Substitution

$$(8)\qquad \begin{cases} y = A_0{}^0 x + A_1{}^0 x' + A_2{}^0 x'' \\ y' = A_0{}' x + A_1{}' x' + A_2{}' x'' \\ y'' = A_0{}'' x + A_1{}'' x' + A_2{}'' x'' \end{cases}$$

in f über. Hiermit ist die algebraische Aequivalenz der Formen definirt. In der Arithmetik der Formen werden aber die Coefficienten, wie der Formen, so auch der Substitutionen als ganzzahlig vorausgesetzt, daher ist die arithmetische Aequivalenz zweier Formen f und f_1 enger darin ausgesprochen, dass f in f_1 durch eine *ganzzahlige* Substitution mit dem Modulus 1 übergeführt werden kann; wo dann, da auch die Coefficienten der umgekehrten Substitution ganzzahlig sein werden, auch f_1 in f durch eine solche Substitution übergeht. Die Formeln (27) vorigen Capitels, welche einer solchen Substitution entsprechen, lehren dann zuerst, dass auch die Coefficienten der Form f_1 ganzzahlig

sein werden. Da aber ihre rechten Seiten homogene lineare Funktionen der Coefficienten a, a', a'', b, b', b'' sind, zeigen sie weiter, dass jeder gemeinsame Theiler der letzteren auch gemeinsamer Theiler aller Coefficienten $a_1, a_1', a_1'', b_1, b_1', b_1''$ sein muss; und da dies wegen der Aequivalenz der beiden Formen auch umgekehrt werden kann, so werden jene sechs Coefficienten denselben grössten gemeinsamen Theiler haben wie diese. Betrachtet man endlich statt der Ausdrücke für b_1, b_1', b_1'' diejenigen für $2b_1, 2b_1', 2b_1''$, so zeigen sich $a_1, a_1', a_1'', 2b_1, 2b_1', 2b_1''$ als homogene lineare Funktionen von $a, a', a'', 2b, 2b', 2b''$ und man erschliesst in gleicher Weise, dass jene denselben grössten gemeinsamen Theiler haben müssen, wie diese. Hieraus aber folgt augenscheinlich, dass, wenn f eine primitive Form ist, jede ihr äquivalente Form es auch ist, und zwar eigentlich oder uneigentlich, je nachdem f eigentlich- oder uneigentlich-primitiv ist.

Bemerkt man ferner, dass nach den Sätzen in nr. 4 vorigen Capitels die Adjungirten F und F_1 zweier Formen f und f_1, welche in arithmetischem Sinne äquivalent sind, dies gleichfalls sein werden, so ist aus dem eben Gesagten ersichtlich, dass der grösste gemeinsame Theiler aller Coefficienten von F_1 dieselbe Zahl Ω sein muss, wie bei F, mit andern Worten, dass äquivalente Formen zur selben Ordnung gehören.

Aus der Definition der Aequivalenz — die wir fortan stets in arithmetischem Sinne verstehen — folgt ohne weiteres, dass zwei Formen, welche derselben dritten Form äquivalent sind, es auch unter einander sind. Alle Formen also, welche einer gegebenen Form äquivalent sind, bilden auch eine Gesammtheit von unter einander äquivalenten Formen von der Art, dass keine andere Form mehr mit einer von ihnen äquivalent sein kann. Man nennt eine solche Gesammtheit von Formen eine Classe von Formen mit der gemeinsamen Determinante. Die voraufgehende Bemerkung lässt sich dann so fassen: dass alle Formen einer Classe derselben Ordnung angehörig sind.

Dies veranlasst eine sehr interessante Bemerkung. Während nämlich in algebraischem Sinne bei den ternären quadra-

tischen Formen nur eine Invariante d. i. nur eine Funktion von den Coefficienten der Form vorhanden ist, die für alle Formen einer Classe denselben Werth hat: die Determinante, sind *in arithmetischer Beziehung zwei* solche Invarianten zu unterscheiden: die beiden Grössen Ω und Δ, und die Determinante erweist sich nur als eine aus diesen beiden *abgeleitete* Invariante der Form. Dasselbe wird sich bei quadratischen Formen mit mehr als drei Veränderlichen noch in reicherer Weise wiederholen. In Rücksicht darauf darf man die Gesammtheit der Formen einer Ordnung (Ω, Δ) als das Analogon zur Gesammtheit aller Formen derselben Determinante bei den binären Formen, wo es eben nur eine Ordnung giebt, betrachten.

3. Es ist wichtig, von vornherein zu beweisen, dass die Anzahl der verschiedenen Classen von Formen der Ordnung (Ω, Δ) nur eine endliche sein kann. Die Methode, welche zum Beweise dieses Satzes sowie des ähnlichen Satzes in allgemeineren Fällen führt, ist die sogenannte Reduktion der Formen.

Die Umstände, welche zur allgemeinen Entwicklung derselben erforderlich sind oder sich an sie knüpfen, machen für sich ein besonderes und ganz eigenartiges Gebiet der Arithmetik der quadratischen Formen aus, dessen zusammenhängende Darstellung im dritten Abschnitt unseres Werkes gegeben wird. Für die beiden ersten Abschnitte bedarf man aus diesem Gebiete fast nur des hier behaupteten Satzes; wir verweisen hinsichtlich desselben auf den dritten Abschnitt, wollen jedoch der Vollständigkeit wegen hier diejenige Art der Reduktion mittheilen, welche in der Theorie der ternären Formen von Gauss für den gedachten Zweck benutzt worden ist.

Wendet man auf die Form $f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ mit der Adjungirten $F = \begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$ die Substitution

$$(9) \qquad x = \alpha y + \beta y', \; x' = \alpha' y + \beta' y', \; x'' = y''$$

an, in welcher $\alpha\beta' - \alpha'\beta = 1$ sei, so geht sie in eine äquivalente Form über, deren erster Coefficient

$$(10) \qquad a\alpha^2 + 2b''\alpha\alpha' + a'\alpha'^2$$

und in deren Adjungirter der dritte Coefficient gleich A'' ist. Die Werthe α, α' können aber bekanntlich — und zwar als relative Primzahlen — so gewählt werden, dass die quadratische Form (10), deren Determinante gleich $-A''$ ist, falls $A'' = 0$ ist, gleich Null, falls aber A'' von Null verschieden, nicht grösser wird als $\sqrt{\mp \frac{4}{3} A''}$; es ist daher möglich, die Substitution (9) so zu bestimmen, dass der erste Coefficient, wenn nicht bereits in der ursprünglichen Form f, so doch in der neuen Form Null oder numerisch nicht grösser als $\sqrt{\mp \frac{4}{3} A''}$ ist, während der dritte Coefficient der Adjungirten ungeändert bleibt.

Behält man für die neue Form und ihre Adjungirte der Einfachheit wegen wieder die ursprüngliche Bezeichnung bei und wendet nunmehr die Substitution

$$(11) \qquad x = y,\ x' = \beta'y' + \gamma'y'',\ x'' = \beta''y' + \gamma''y'',$$

in welcher $\beta'\gamma'' - \beta''\gamma' = 1$ sei, auf f an, so verwandelt sich diese Form wieder in eine äquivalente Form, deren erster Coefficient ungeändert geblieben ist, während der dritte Coefficient ihrer Adjungirten in

$$A'\beta''^2 - 2B\beta'\beta'' + A''\beta'^2$$

übergeht und durch geeignete Wahl der relativ primen Zahlen β', β'' und folglich der Substitution (11), falls die Determinante $B^2 - A'A'' = -Da$ dieser quadratischen Form also a verschwindet, gleich Null, im entgegengesetzten Falle numerisch nicht grösser als $\sqrt{\pm \frac{4}{3} Da}$ gemacht werden kann.

Indem man diese Betrachtung abwechselnd wiederholt, wird sowohl die Reihe der ersten Coefficienten der Formen als die Reihe der dritten Coefficienten ihrer Adjungirten eine Reihe ganzer Zahlen sein, die abwechselnd gleich sind und kleiner werden; nothwendig wird also endlich weder durch das erste noch durch das zweite Verfahren eine weitere Vereinfachung mehr herbeizuführen und dann also entweder die Coefficienten a, A'' beide gleich Null oder beide

von Null verschieden aber zugleich in numerischem Sinne

$$a^2 \gtreqless \frac{4}{3} A'', \qquad A''^2 \gtreqless \frac{4}{3} Da$$

folglich

(12) $$a \gtreqless \frac{4}{3} \sqrt[3]{D}, \qquad A'' \gtreqless \frac{4}{3} \sqrt[3]{D^2}$$

sein. — Wendet man dann aber die Substitution

$$x = y + \beta y' + \gamma y'',\ x' = y' + \gamma' y'',\ x'' = y''$$

an, so geht die Form f in eine äquivalente Form $\begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$ mit der Adjungirten $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$ über, in welcher

$$\begin{aligned} m &= a,\ m' = a' + 2b''\beta + a\beta^2 \\ m'' &= a'' + 2b\gamma' + 2b'\gamma + a\gamma^2 + 2b''\gamma\gamma' + a'\gamma'^2 \\ n &= b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma \\ n' &= b' + a\gamma + b''\gamma',\ n'' = b'' + a\beta \\ M'' &= A'',\ N = B - A''\gamma',\ N' = B' - N\beta - A''\gamma \end{aligned}$$

ist. Sind nun erstens a, A'' nicht Null, so lassen sich β, γ', γ so wählen, dass, während $m = a$ und $M'' = A''$ ist, n'' num. $\gtreqless \frac{a}{2}$, N und N' num. $\gtreqless \frac{A''}{2}$ werden.

Sind zweitens a, A'' und folglich auch b'' gleich Null, so wird

$$m = 0,\ m' = a',\ n' = b',\ n'' = 0$$

also

(13) $$-D = a'b'^2 = m'n'^2,$$

und $n = b + a'\gamma' + b'\beta$ kann num. $\gtreqless$ als der grösste gemeinsame Theiler von a', b', und

$$m'' = a'' + 2b\gamma' + a'\gamma'^2 + 2b'\gamma \text{ num.} \gtreqless b'$$

gemacht werden. Der so beschränkten Formen giebt es aber nur eine endliche Menge. Denn im zweiten Falle hat b' oder n' wegen (13) und folglich auch a' oder m' nur eine endliche Anzahl von Werthen, also auch n und m'' nur eine solche. Im ersten Falle dagegen giebt es nur eine endliche Menge zulässiger Werthsysteme für die Coefficienten m, M'', n'', N, N';

legt man aber diesen Coefficienten eins der gedachten Werthsysteme bei, so finden sich daraus unmittelbar die etwa zugehörigen Zahlen m', N'', M' durch die Formeln

$$m' = \frac{n''^2 + M''}{m}, \quad N'' = \frac{-n''D + NN'}{M''}, \quad M' = \frac{N^2 + Dm}{M''}$$

und sodann die etwa zugehörigen M, n, n', m'' durch die Formeln

$$M = \frac{N'^2 + Dm'}{M''}, \quad n = \frac{-MN + N'N''}{D}, \quad n' = \frac{-M'N' + N''N}{D}$$

$$m'' = \frac{n'^2 + M'}{m} = \frac{-N'' + nn'}{n''} = \frac{n^2 + M}{m'},$$

und nur denjenigen jener Werthsysteme, für welche diese Formeln **ganzzahlige** Werthe der Coefficienten liefern, entsprechen zulässige Formen.

Aus diesen Betrachtungen geht aber hervor, dass jede ternäre quadratische Form mit der Determinante D also auch jede solche der Ordnung (Ω, Δ) mit einer dieser nur in endlicher Anzahl vorhandenen Formen äquivalent ist, und **folglich kann auch die Anzahl der nicht äquivalenten Classen von Formen dieser Ordnung nur eine endliche sein.**

4. Wird die Form f durch eine ganzzahlige Substitution (7) in eine Form f_1 verwandelt, der Art, dass die Gleichung

$$(14) \qquad f(x, x', x'') = f_1(y, y', y'')$$

identisch stattfindet, wenn x, x', x'' mit y, y', y'' durch jene Gleichungen verbunden sind, so wird auch die folgende erfüllt sein:

$$(15) \qquad f(x, x', x'') = a_1 y^2 + 2b_1'' yy' + a_1' y'^2,$$

wenn

$$(16) \qquad \begin{cases} x = \alpha_0^0 y + \alpha_0' y' \\ x' = \alpha_1^0 y + \alpha_1' y' \\ x'' = \alpha_2^0 y + \alpha_2' y' \end{cases}$$

gesetzt wird. Man sagt alsdann: **Die binäre quadratische Form (a_1, b_1'', a_1') werde mittels der Formeln (16) durch die ternäre quadratische Form f dargestellt,** und die Darstellung wird **eine eigentliche** genannt, **wenn die drei**

ganzen Zahlen

(17) $$\alpha_1^0\alpha_2' - \alpha_2^0\alpha_1', \quad \alpha_2^0\alpha_0' - \alpha_0^0\alpha_2', \quad \alpha_0^0\alpha_1' - \alpha_1^0\alpha_0'$$

keinen von 1 verschiedenen Theiler haben.

In gleicher Weise wird

$$f(x, x', x'') = a_1 y^2$$

sein, wenn man setzt

$$x = \alpha_0^0 y, \quad x' = \alpha_1^0 y, \quad x'' = \alpha_2^0 y$$

oder einfacher

(18) $$f(\alpha_0^0, \alpha_1^0, \alpha_2^0) = a_1.$$

Diese Gleichung meint man, wenn man sagt, die Zahl a_1 werde mittels der Werthe $\alpha_0^0, \alpha_1^0, \alpha_2^0$ durch die ternäre Form f dargestellt. Die Darstellung heisst zudem eine eigentliche, wenn die darstellenden Zahlen $\alpha_0^0, \alpha_1^0, \alpha_2^0$ keinen von 1 verschiedenen gemeinsamen Theiler haben.

Während also bei den binären Formen nur die Darstellung von Zahlen in Frage kommt, tritt bei den Formen mit drei Veränderlichen noch eine andere Darstellung, die von (binären) Formen auf, und noch allgemeiner verhalten sich die Formen mit mehr Veränderlichen.

Leicht ist zu übersehen, dass äquivalente ternäre Formen stets dieselben Zahlen eigentlich darstellen. Man bemerke vorweg, dass, wenn x, x', x'' mit y, y', y'' durch eine ganzzahlige Substitution (7) verbunden sind, deren Modulus 1 ist, jedem ganzzahligen Systeme y, y', y'' auch ein ganzzahliges System x, x', x'' und wegen der aufgelösten Gleichungen auch umgekehrt entspricht; auch wird y, y', y'' ein primitives System sein — darunter soll abkürzend stets ein solches verstanden werden, dessen Zahlen keinen von 1 verschiedenen gemeinsamen Theiler haben — wenn x, x', x'' ein solches ist, und auch umgekehrt. Besteht hiernach die Gleichung (14) für die durch (7) mit einander verbundenen Systeme d. h. sind f und f_1 äquivalent, so wird jede Zahl, welche mittels eines primitiven Systems x, x', x'' also eigentlich durch f dargestellt wird, durch das entsprechende System y, y', y'' also eigentlich auch durch f_1 dargestellt werden, und umgekehrt.

Desgleichen stellen äquivalente ternäre Formen auch stets dieselben binären Formen eigentlich dar. Denn, wird die Form

$$(15a)\qquad a_1 y^2 + 2b_1'' yy' + a_1' y'^2$$

mittels der Formeln (16) eigentlich durch die Form $f(x, x', x'')$ dargestellt, so kann man, da dann die drei Zahlen (17) keinen von 1 verschiedenen gemeinsamen Theiler haben, drei ganze Zahlen $\alpha_0'', \alpha_1'', \alpha_2''$ der Art wählen*), dass die Gleichung

$$(\alpha_1^0\alpha_2' - \alpha_2^0\alpha_1')\alpha_0'' + (\alpha_2^0\alpha_0' - \alpha_0^0\alpha_2')\alpha_1'' + (\alpha_0^0\alpha_1' - \alpha_1^0\alpha_0')\alpha_2'' = 1$$

erfüllt, d. h. dass der Modulus der Substitution (7) gleich 1 ist. Durch diese ganzzahlige Substitution geht also $f(x, x', x'')$ in eine äquivalente Form $f_1(y, y', y'')$ über, von welcher die Form (15a) ein Bestandtheil ist. Ist aber $\varphi(z, z', z'')$ eine Form, welche äquivalent ist mit $f(x, x', x'')$, so ist sie es auch mit $f_1(y, y', y'')$ und es giebt folglich eine ganzzahlige Substitution

$$\begin{aligned} z &= \beta_0^0 y + \beta_0' y' + \beta_0'' y'' \\ z' &= \beta_1^0 y + \beta_1' y' + \beta_1'' y'' \\ z'' &= \beta_2^0 y + \beta_2' y' + \beta_2'' y'' \end{aligned}$$

mit dem Modulus 1, für welche

$$\varphi(z, z', z'') = f_1(y, y', y'')$$

wird. Die Form (15a) wird daher auch durch $\varphi(z, z', z'')$ dargestellt, indem man setzt

$$\begin{aligned} z &= \beta_0^0 y + \beta_0' y' \\ z' &= \beta_1^0 y + \beta_1' y' \\ z'' &= \beta_2^0 y + \beta_2' y', \end{aligned}$$

und diese Darstellung ist eine eigentliche, denn da die Gleichung besteht:

$$(\beta_1^0\beta_2' - \beta_2^0\beta_1')\beta_0'' + (\beta_2^0\beta_0' - \beta_0^0\beta_2')\beta_1'' + (\beta_0^0\beta_1' - \beta_1^0\beta_0')\beta_2'' = 1,$$

können die drei Zahlen

$$\beta_1^0\beta_2' - \beta_2^0\beta_1', \quad \beta_2^0\beta_0' - \beta_0^0\beta_2', \quad \beta_0^0\beta_1' - \beta_1^0\beta_0'$$

keinen von 1 verschiedenen gemeinsamen Theiler haben.

---

*) S. hierzu 2. Abschnitt, 3. Cap. nr. 5.

5. Nicht jede Zahl kann durch eine gegebene ternäre Form dargestellt werden. Während wir das Problem der Darstellung selbst erst später behandeln werden, müssen hier einige allgemeine Bemerkungen vorausgeschickt werden.

Erinnert man sich zunächst der Unterscheidung aller Formen in bestimmte (positive) und in unbestimmte Formen, so ist ersichtlich, dass durch die erstern nur positive ganze Zahlen darstellbar sind, während das Vorzeichen der durch letztere darstellbaren Zahlen sowohl positiv als negativ sein kann.

Sei ferner N eine beliebig gegebene Zahl und $f(x, x', x'')$ zunächst eine eigentlich-primitive Form. Bedeutet dann p irgend eine Primzahl, so können die Zahlen $a, a', a'', 2b, 2b', 2b''$ nicht sämmtlich durch p theilbar sein; ist eine der Zahlen a, a', a'', z. B. a, nicht theilbar durch p, so wird auch die Form nicht theilbar durch p, wenn man x', x'' theilbar, x nicht theilbar wählt durch p; sind alle drei Zahlen a, a', a'' theilbar durch p, so darf eine der Zahlen $2b, 2b', 2b''$, z. B. $2b$, es nicht sein, und dann nimmt die Form einen durch p nicht aufgehenden Werth an, wenn man x durch p theilbar, x', x'' nicht theilbar wählt. So kann man immer erreichen, dass $f(x, x', x'')$ durch p nicht theilbar wird. Da aber diese Bedingungen der Theilbarkeit resp. Nichttheilbarkeit der Zahlen x, x', x'' in Bezug auf beliebig viel verschiedene, z. B. in Bezug auf die in N aufgehenden Primzahlen stets gleichzeitig erfüllbar sind, ergiebt sich der Satz: Durch eine eigentlich-primitive Form können stets Zahlen dargestellt werden, welche zu einer beliebig gegebenen Zahl prim sind. Diese Darstellung darf sogar als eine eigentliche gedacht werden, da die Form, wenn sie prim zu N wird für Werthe x, x', x'', welche einen gemeinsamen Theiler haben, es auch bleiben wird, wenn man diesen gemeinsamen Theiler unterdrückt.

Bei einer uneigentlich primitiven Form sind $\frac{a}{2}, \frac{a'}{2}, \frac{a''}{2}$ ganze Zahlen, welche zusammen mit b, b', b'' keinen gemeinsamen Theiler haben. Hier wird also von $\frac{1}{2} f(x, x', x'')$ genau dasselbe gelten wie vorher von $f(x, x', x'')$ und man erhält

den Satz: Durch eine uneigentlich-primitive Form kann stets das Doppelte einer Zahl (eigentlich) dargestellt werden, die zu einer beliebig gegebenen Zahl prim ist.

Sind, wie angenommen, die Determinante also auch die beiden Zahlen Ω, Δ ungerade, so kommen nur eigentlich-primitive Formen in Betracht. Unter derselben Voraussetzung sind dann durch die Form $f(x, x', x'')$ Zahlen von jeder der beiden Linearformen $4\varkappa + 1$ und $4\varkappa + 3$, also sowohl quadratische Reste als Nichtreste (mod. 4) darstellbar. Denn einer der Coefficienten a, a', a'', z. B. a ist sicher ungerade; macht man dann die Substitution

$$x = y + \lambda y' + \mu y'', \quad x' = y', \quad x'' = y'',$$

so geht $f(x, x', x'')$ in eine äquivalente Form

$$f_1 = a_1 y^2 + a_1' y'^2 + a_1'' y''^2 + 2b_1 y' y'' + 2b_1' y'' y + 2b_1'' y y'$$

über, in welcher

$$a_1 = a, \quad a_1' = a\lambda^2 + 2b''\lambda + a', \quad a_1'' = a\mu^2 + 2b'\mu + a''$$

ist; die drei Coefficienten a_1, a_1', a_1'' werden also ungerade sein, wenn man λ resp. μ gerade oder ungerade wählt, je nachdem a' resp. a'' ungerade oder gerade ist; nach der Gleichung

$$D = a_1 a_1' a_1'' + 2b_1 b_1' b_1'' - a_1 b_1^2 - a_1' b_1'^2 - a_1'' b_1''^2$$

ergiebt sich alsdann $b_1 + b_1' + b_1''$ gerade also

$$a_1 + a_1' + a_1'' + 2(b_1 + b_1' + b_1'') \equiv a_1 + a_1' + a_1'' \pmod{4}.$$

Letztere Zahl aber ist, wie die Zahlen a_1, a_1', a_1'', eine der durch f_1 also auch durch f darstellbaren Zahlen und würde, wenn alle Zahlen a_1, a_1', a_1'' die gleiche Linearform hätten, die entgegengesetzte haben.

Offenbar wird es nun auch möglich sein, x, x', x'' so zu wählen, dass die eigentlich-primitive Form $f(x, x', x'')$ einen Werth erhält, welcher zu einer beliebig gegebenen Zahl N prim und von einer bestimmten der beiden Linearformen $4\varkappa + 1$, $4\varkappa + 3$ ist. Man darf ihn sogar noch positiv voraussetzen. Dies ist von selbst einleuchtend, wenn die Form positiv ist; ist sie unbestimmt, so darf man doch a positiv voraussetzen, indem man nöthigenfalls (vgl. nr. 8) die Form f durch eine äquivalente ersetzt, deren erster Coefficient positiv ist. Sei dann

$$x = \alpha, \quad x' = \alpha', \quad x'' = \alpha''$$

ein Werthsystem, für welches f den andern vorher angegebenen Bedingungen genügt; dann wird auch

$$x = \alpha + 4Nz, \quad x' = \alpha', \quad x'' = \alpha''$$

ein solches sein, aus der Gleichung

$$a \cdot f(\alpha + 4Nz, \alpha', \alpha'')$$

$$= [a(\alpha + 4Nz) + b''\alpha' + b'\alpha'']^2 + A'\alpha''^2 - 2B\alpha''\alpha' + A''\alpha'^2$$

ersieht man aber, dass für ein hinreichend grosses z die Form f auch positiv werden muss.

6. Es giebt aber andere Moduln, in Bezug auf welche der quadratische Charakter der Zahlen, welche eine ternäre Form darstellen kann, nicht willkürlich ist, und auf diesem Umstande, der sich schon in der Lehre von den binären quadratischen Formen herausgestellt, beruht, wie bei jenen, die Vertheilung aller ternären Formen einer bestimmten Ordnung in Geschlechter. Man begründet dieselbe am einfachsten auf die beiden Grundformeln, welche bei den angenommenen Bezeichnungen jetzt folgende Gestalt erhalten:

$$(19) \quad \begin{cases} f(x, x', x'') \cdot f(y, y', y'') \\ = (yf^0(x) + y'f^1(x) + y''f^2(x))^2 \\ + \Omega \cdot \mathfrak{F}(x'y'' - x''y', x''y - xy'', xy' - x'y) \end{cases}$$

und

$$(20) \quad \begin{cases} \mathfrak{F}(x, x', x'') \cdot \mathfrak{F}(y, y', y'') \\ = (y\mathfrak{F}^0(x) + y'\mathfrak{F}^1(x) + y''\mathfrak{F}^2(x))^2 \\ + \Delta \cdot f(x'y'' - x''y', x''y - xy'', xy' - x'y). \end{cases}$$

Versteht man nämlich unter ω irgend einen Primfaktor von Ω und ertheilt den Veränderlichen x, x', x''; y, y', y'' solche Werthe, für welche die Form f nicht theilbar wird durch ω, so ergiebt sich aus der ersten dieser Formeln unmittelbar

$$\left(\frac{f(x, x', x'')}{\omega}\right) = \left(\frac{f(y, y', y'')}{\omega}\right)$$

d. h. für alle ganzzahligen Werthe der Form f, welche nicht theilbar sind durch ω, hat das Legendre'sche Symbol $\left(\frac{f}{\omega}\right)$ ein- und denselben Werth, sie sind folglich entweder sämmt-

lich quadratische Reste oder sämmtlich quadratische Nichtreste von ω. Mithin hat die Form bezüglich des Primfaktors ω einen durch den Werth des Symbols $\left(\frac{f}{\omega}\right)$ bestimmten quadratischen Charakter.

Bezeichnet man dagegen mit δ irgend einen Primfaktor von Δ und wählt die Unbestimmten x, x', x''; y, y', y'' der Art, dass der Werth der Form $\mathfrak{F}$ nicht durch δ aufgeht, so folgt in gleicher Weise aus der zweiten der obigen Formeln

$$\left(\frac{\mathfrak{F}(x, x', x'')}{\delta}\right) = \left(\frac{\mathfrak{F}(y, y', y'')}{\delta}\right),$$

für alle ganzzahligen Werthe der Reciproken $\mathfrak{F}$, welche nicht theilbar sind durch δ, hat also das Legendre'sche Symbol $\left(\frac{\mathfrak{F}}{\delta}\right)$ ein- und denselben Werth. Mithin kommt der Form f bezüglich des Primfaktors δ ein durch den Werth des Symbols $\left(\frac{\mathfrak{F}}{\delta}\right)$ bestimmter quadratischer Charakter zu.

Demnach sind der Form f so viel verschiedene Einzelcharaktere eigen, als die Anzahl aller ω und aller δ beträgt. Da Ω, Δ gemeinsame Primfaktoren haben können, sollen fortan mit $\omega, \omega', \omega'', \ldots$ alle in Ω aber nicht in Δ, mit $\delta, \delta', \delta'' \ldots$ alle in Δ aber nicht in Ω, und mit $r, r', r'', \ldots$ alle sowohl in Ω als in Δ aufgehende Primzahlen bezeichnet werden. Dann sind die sämmtlichen Einzelcharaktere der Form f durch die Werthe der folgenden Symbole:

$$(21) \qquad \begin{cases} \left(\frac{f}{\omega}\right), \left(\frac{f}{\omega'}\right), \cdots \left(\frac{f}{r}\right), \left(\frac{f}{r'}\right), \cdots \\ \left(\frac{\mathfrak{F}}{\delta}\right), \left(\frac{\mathfrak{F}}{\delta'}\right), \cdots \left(\frac{\mathfrak{F}}{r}\right), \left(\frac{\mathfrak{F}}{r'}\right), \cdots \end{cases}$$

bestimmt und letztere definiren zusammengenommen *den Charakter* der Form f.

Alle Formen derselben Ordnung, welche gleichen Charakter haben, bilden ein Geschlecht von Formen. Da Formen derselben Classe stets dieselben Zahlen darstellen, müssen sie offenbar auch gleichen Charakter haben; Formen derselben Classe gehören mithin auch immer demselben Geschlechte an. Ist μ, ν, ϱ resp. die Anzahl aller Zahlen ω, δ, r, so ist die Anzahl der sämmtlichen Einzel-

charaktere (21), deren jeder den Werth $+1$ oder -1 haben kann, gleich $\mu + \nu + 2\varrho$, und demnach die Anzahl aller möglichen Zeichencombinationen d. h. die Anzahl aller überhaupt denkbaren Geschlechter der Ordnung (Ω, Δ) gleich

$$2^{\mu+\nu+2\varrho}.$$

Ob diese Geschlechter aber auch wirklich vorhanden sind d. i. ob jeder möglichen Zeichencombination auch wirklich ternäre Formen jener Ordnung zugehören, wird später sich entscheiden.

7. Diese wichtigen Ergebnisse sollen von einer anderen, allgemeineren Grundlage aus noch einmal hergeleitet werden. Wir stützen uns dazu auf einen Satz, welchen zuerst Stephen Smith aufgestellt hat und der uns auch weiter noch dienlich sein wird, folgen aber beim Beweise desselben mehr dem Gedankengange von Minkowski*). Der Satz lautet folgendermassen:

Ist $f(x, x', x'')$ eine eigentlich-primitive Form mit ungerader Determinante, N aber eine beliebig gegebene Zahl, so kann in der Classe von f stets eine Form φ mit der Reciproken Φ gefunden werden, für welche die Congruenzen

$$(22) \quad \left.\begin{cases} \varphi \equiv \alpha x^2 + \alpha'\Omega x'^2 + \alpha''\Omega\Delta x''^2 \\ \Phi \equiv \alpha'\alpha''\Omega\Delta x^2 + \alpha''\alpha\Delta x'^2 + \alpha\alpha' x''^2 \\ 1 \equiv \alpha\alpha'\alpha'' \end{cases}\right\} \pmod{N}$$

erfüllt sind, Congruenzen, welche den Sinn haben sollen, dass rechts und links die Coefficienten sowohl der Quadrate wie auch der doppelten Produkte der Veränderlichen resp. einander congruent sind.

---

*) S. die vortreffliche Abhandlung von Henry Stephen Smith in Philos. Transactions of the Royal Society of London for the year 1867: On the Orders and Genera of Ternary Quadratic Forms, sowie H. Minkowski's Preisschrift: Mémoire sur la théorie des formes quadratiques à coefficiens entiers, in Mém. prés. p. div. Savants Etr. t. 29. — Da beide Mathematiker die Frage nach den Ordnungen und Geschlechtern der quadratischen Formen ganz allgemein, ohne beschränkende Voraussetzungen über die Determinante behandeln, verweisen wir überhaupt den Leser, welcher eine Ergänzung des im Texte Gebotenen sucht, auf diese Abhandlungen.

Den Betrachtungen, durch welche dieser Satz begründet werden soll, sei der Beweis eines Hilfssatzes vorausgeschickt, welchen zuerst Gauss (Disquis. Arithm. art. 279) unter der Form einer Aufgabe hergeleitet hat. Sind nämlich Z, Z', Z'' drei ganze Zahlen ohne einen von 1 verschiedenen gemeinsamen Theiler, so können sechs andere ganze Zahlen x, x', x'', y, y', y'' so gewählt werden, dass

$$x'y'' - x''y' = Z,\ x''y - xy'' = Z',\ xy' - x'y = Z''.$$

In der That lassen sich zunächst ganze Zahlen x, x', x'' ohne einen von 1 verschiedenen gemeinsamen Theiler, die nicht sämmtlich verschwinden, so angeben, dass

$$Zx + Z'x' + Z''x'' = 0 \tag{23}$$

wird; man braucht zu diesem Zwecke z. B. nur

$$x = zZ'',\ x' = z'Z'',\ x'' = -zZ - z'Z'$$

zu setzen, wo z, z' beliebige ganze Zahlen sind, und diese Zahlen x, x', x'' von ihrem grössten gemeinsamen Theiler zu befreien. Aus einer Lösung x, x', x'' der Gleichung (23) ergeben sich aber unendlich viel andere, wenn man, unter λ, μ, ν beliebige ganze Zahlen verstehend,

$$y = x - \mu Z'' + \nu Z',\ y' = x' - \nu Z + \lambda Z'',\ y'' = x'' - \lambda Z' + \mu Z$$

setzt. Mittels dieser Formeln erschliesst man leicht

$$x'y'' - x''y' = -\lambda(Zx + Z'x' + Z''x'') + Z(\lambda x + \mu x' + \nu x'')$$

d. i. mit Rücksicht auf (23)

$$x'y'' - x''y' = Z(\lambda x + \mu x' + \nu x'')$$

und ähnlich

$$x''y - xy'' = Z'(\lambda x + \mu x' + \nu x'')$$
$$xy' - x'y = Z''(\lambda x + \mu x' + \nu x'').$$

Wählt man nun, was bekanntlich möglich ist*), die unbestimmten ganzen Zahlen λ, μ, ν der Art, dass

$$\lambda x + \mu x' + \nu x'' = 1$$

wird, so findet sich, wie es sein sollte,

$$x'y'' - x''y' = Z,\ x''y - xy'' = Z',\ xy' - x'y = Z''. \tag{24}$$

Zu späterer Verwendung werde noch gezeigt, wie

---

*) S. Abschnitt II, 3. Cap. nr. 5.

man aus einer Lösung x, x', x'', y, y', y'' der Aufgabe alle Lösungen derselben herleiten kann. Sei noch

$$(25) \qquad \xi'\eta'' - \xi''\eta' = Z, \ \xi''\eta - \xi\eta'' = Z', \ \xi\eta' - \xi'\eta = Z''.$$

Man bestimme drei ganze Zahlen z, z', z'' der Art, dass

$$Zz + Z'z' + Z''z'' = 1$$

oder

$$\begin{vmatrix} x & y & z \\ x' & y' & z' \\ x'' & y'' & z'' \end{vmatrix} = 1$$

wird. Nennt man dann

$$\begin{vmatrix} X & Y & Z \\ X' & Y' & Z' \\ X'' & Y'' & Z'' \end{vmatrix}$$

die adjungirte Determinante, so bestehen die Beziehungen

$$x = Y'Z'' - Y''Z', \quad y = X''Z' - X'Z'',$$

denen man mit Rücksicht auf (25) leicht folgende Gestalt giebt:

$$(26) \qquad x = \delta\xi - \gamma\eta, \ y = -\beta\xi + \alpha\eta,$$

wenn zur Abkürzung

$$X\xi + X'\xi' + X''\xi'' = \alpha, \quad X\eta + X'\eta' + X''\eta'' = \beta$$
$$Y\xi + Y'\xi' + Y''\xi'' = \gamma, \quad Y\eta + Y'\eta' + Y''\eta'' = \delta$$

gesetzt wird. Hieraus schliesst man mittels der Determinantenformel in nr. 2 des ersten Capitels und mit Rücksicht auf (25)

$$\alpha\delta - \beta\gamma$$
$$= (X'Y'' - X''Y')Z + (X''Y - XY'')Z' + (XY' - X'Y)Z'' = 1$$

und nun aus (26)

$$\xi = \alpha x + \gamma y, \quad \eta = \beta x + \delta y$$

und in analoger Weise

$$(27) \qquad \left.\begin{aligned} \xi' &= \alpha x' + \gamma y', \quad \eta' = \beta x' + \delta y' \\ \xi'' &= \alpha x'' + \gamma y'', \quad \eta'' = \beta x'' + \delta y''. \end{aligned}\right\}$$

Alle Lösungen der Aufgabe finden sich also aus einer von ihnen mittels dieser Formeln (27), wenn man darin für $\alpha, \beta, \gamma, \delta$ alle möglichen ganzen Zahlen setzt, welche die Gleichung

$$\alpha\delta - \beta\gamma = 1$$

erfüllen; auch leuchtet ein, dass jedem solchen Systeme ganzer Zahlen $\alpha, \beta, \gamma, \delta$ eine Lösung entspricht, da aus jenen Formeln sogleich die folgenden:

$$\xi'\eta''-\xi''\eta'=(x'y''-x''y')(\alpha\delta-\beta\gamma)=x'y''-x''y'$$

und analog

$$\xi''\eta-\xi\eta''=x''y-xy'', \quad \xi\eta'-\xi'\eta=xy'-x'y$$

hervorgehen.

8. Dies vorausgeschickt, wenden wir uns nun zur Herleitung der Congruenzen (22). Sei $N'=4ND$. Dem in nr. 5 Bewiesenen zufolge kann durch f eine Zahl α eigentlich dargestellt werden, welche prim ist gegen N' und der Congruenz $\alpha\Delta\equiv 1 \pmod{4}$ genügt, und es sei

$$f(\alpha_0^0, \alpha_1^0, \alpha_2^0)=\alpha,$$

wobei $\alpha_0^0, \alpha_1^0, \alpha_2^0$ ein primitives System bilden. Man kann dann ganze Zahlen $\alpha_0', \alpha_1', \alpha_2', \alpha_0'', \alpha_1'', \alpha_2''$ der Art wählen, dass die Substitution

$$\begin{aligned} x &= \alpha_0^0 y + \alpha_0' y' + \alpha_0'' y'' \\ x' &= \alpha_1^0 y + \alpha_1' y' + \alpha_1'' y'' \\ x'' &= \alpha_2^0 y + \alpha_2' y' + \alpha_2'' y'' \end{aligned}$$

den Modulus 1 erhält. In der That erreicht man dies, wenn man zunächst solche ganze Zahlen $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ bestimmt, dass

$$\alpha_0^0\mathsf{A}+\alpha_1^0\mathsf{A}'+\alpha_2^0\mathsf{A}''=1$$

ist, und darauf die Zahlen $\alpha_0', \alpha_1', \alpha_2', \alpha_0'', \alpha_1'', \alpha_2''$ so, dass

$$\alpha_1'\alpha_2''-\alpha_1''\alpha_2'=\mathsf{A}, \quad \alpha_2'\alpha_0''-\alpha_2''\alpha_0'=\mathsf{A}', \quad \alpha_0'\alpha_1''-\alpha_0''\alpha_1'=\mathsf{A}''$$

wird, was dem Hilfssatze gemäss geschehen kann. Durch diese Substitution aber verwandelt sich f in eine äquivalente Form

$$\alpha y^2+a'y'^2+a''y''^2+2by'y''+2b'y''y+2b''yy'$$

mit dem ersten Coefficienten α. Die neue Substitution

$$y=z+\lambda z'+\mu z'', \quad y'=z', \quad y''=z''$$

liefert eine andere äquivalente Form

$$(28)\quad f_1=\alpha z^2+a_1'z'^2+a_1''z''^2+2b_1z'z''+2b_1'z''z+2b_1''zz',$$

in welcher

$$b_1'=\alpha\mu+b', \quad b_1''=\alpha\lambda+b''$$

ist, und durch geeignete Wahl der unbestimmten ganzen Zahlen

λ, μ können b_1', b_1'' durch N' theilbar gemacht werden, sodass man schreiben darf

(29) $$f_1 \equiv \alpha z^2 + a_1' z'^2 + a_1'' z''^2 + 2 b_1 z' z'' \pmod{N'}.$$

Hieraus ergeben sich aber, wenn f als eine Form der Ordnung (Ω, Δ) vorausgesetzt wird, wegen der Congruenzen

$$\alpha a_1'' - b_1'^2 \equiv \alpha a_1' - b_1''^2 \equiv b_1' b_1'' - \alpha b_1 \equiv 0 \pmod{\Omega}$$

die Zahlen a_1', a_1'', b_1 theilbar durch Ω, etwa

$$a_1' = \Omega \alpha_1, \quad a_1'' = \Omega \alpha_2, \quad b_1 = \Omega \beta,$$

und somit

(30) $$f_1 \equiv \alpha z^2 + \Omega(\alpha_1 z'^2 + \alpha_2 z''^2 + 2\beta z' z'') \pmod{N'}.$$

Die Zahlen α_1, α_2, β können keinen von 1 verschiedenen gemeinsamen Theiler mehr haben. Denn ein ihnen gemeinsamer Primfaktor p müsste dem Ausdrucke der Determinante zufolge in D aufgehen und die Coefficienten der Adjungirten von (28), nämlich

$$\begin{array}{lll} a_1' a_1'' - b_1^2, & a_1'' \alpha - b_1'^2, & a_1' \alpha - b_1''^2 \\ b_1' b_1'' - \alpha b_1, & b_1'' b_1 - a_1' b_1', & b_1 b_1' - a_1'' b_1'', \end{array}$$

würden dann sämmtlich durch Ωp theilbar sein, gegen die Voraussetzung über die Ordnung von f. Ausserdem können nicht beide Zahlen α_1, α_2 gerade sein, denn dann wäre β ungerade, und da aus dem Ausdrucke der Determinante die Congruenz

$$\Delta \equiv \alpha(\alpha_1 \alpha_2 - \beta^2) \pmod{4 N \Delta}$$

gefolgert wird, so ergäbe sich

$$1 \equiv \alpha \Delta \equiv \alpha_1 \alpha_2 - \beta^2 \equiv -1 \pmod{4},$$

was nicht sein kann.

Die angegebene Beschaffenheit der Coefficienten α_1, α_2, β ermöglicht es, durch die binäre quadratische Form

(31) $$\psi = \alpha_1 z'^2 + \alpha_2 z''^2 + 2\beta z' z''$$

eine Zahl α' eigentlich darzustellen, welche prim ist gegen N'. Ist

$$\alpha_1 \nu'^2 + \alpha_2 \nu''^2 + 2\beta \nu' \nu'' = \alpha'$$

eine solche Darstellung und sind ϱ', ϱ'' zwei ganze Zahlen, welche die Gleichung

$$\nu' \varrho'' - \nu'' \varrho' = 1$$

befriedigen, so geht die Form ψ durch die Substitution

$$z' = \nu' u' + \varrho' u'', \quad z'' = \nu'' u' + \varrho'' u''$$

in eine äquivalente Form

$$\alpha' u'^2 + 2\beta' u' u'' + \gamma u''^2,$$

deren erster Coefficient α' ist, und letztere, wenn

$$u' = x' + \varkappa x'', \quad u'' = x''$$

gesetzt wird, in eine wieder äquivalente Form

$$\chi = \alpha' x'^2 + 2(\beta' + \alpha' \varkappa) x' x'' + \delta x''^2$$

über, deren mittlerer Coefficient $\beta' + \alpha' \varkappa$ durch geeignete Wahl der unbestimmten ganzen Zahl $\varkappa$ durch N' theilbar gemacht werden kann, sodass man für die Form χ die Congruenz

$$\chi \equiv \alpha' x'^2 + \delta x''^2 \pmod{N'}$$

also auch

$$\Omega \chi \equiv \alpha' \Omega x'^2 + \delta \Omega x''^2 \pmod{N'}$$

erhält. — Da sich nun durch dieselbe Reihe von Substitutionen in Verbindung mit $z = x$ die Form f_1 in eine äquivalente Form φ mit dem ersten Coefficienten α verwandelt, wird für letztere die Congruenz

$$\varphi \equiv \alpha x^2 + \alpha' \Omega x'^2 + \delta \Omega x''^2 \pmod{N'} \tag{32}$$

erfüllt sein, aus welcher mit Rücksicht auf den Ausdruck der Determinante die weitere:

$$\Delta \equiv \alpha \alpha' \delta \pmod{4 N \Delta}$$

hervorgeht; diese erfordert, da α, α' zu N' also zu Δ prim sind, dass δ theilbar sei durch Δ, und giebt, wenn demgemäss $\delta = \Delta \alpha''$ gesetzt wird, der Congruenz (32) die folgende Form

$$\varphi \equiv \alpha x^2 + \alpha' \Omega x'^2 + \alpha'' \Omega \Delta x''^2 \pmod{N'};$$

aus ihr gehen diese andern:

$$\left.\begin{aligned} \varphi &\equiv \alpha x^2 + \alpha' \Omega x'^2 + \alpha'' \Omega \Delta x''^2 \\ \Phi &\equiv \alpha' \alpha'' \Omega \Delta x^2 + \alpha'' \alpha \Delta x'^2 + \alpha \alpha' x''^2 \end{aligned}\right\} \pmod{N}$$

hervor, während

$$1 \equiv \alpha \alpha' \alpha'' \pmod{N}$$

gefunden wird, ganz wie der ausgesprochene Satz es behauptet.

9. Versteht man nun unter N das Produkt $\Omega \Delta$, so ergeben sich die Resultate der nr. 6 ganz von selbst.

Denn, indem man hier wieder mit ω, δ jeden Primfaktor von Ω resp. Δ bezeichnet, folgt aus der ersten der Congruenzen (22)

$$\varphi \equiv \alpha x^2 \pmod{\omega},$$

aus der zweiten

$$\Phi \equiv \alpha\alpha' x''^2 \pmod{\delta},$$

während sich aus der dritten α, α' prim sowohl zu ω als zu δ ergeben. Legt man also in der Form φ resp. Φ den Unbestimmten x, x', x'' solche Werthe bei, welche sie durch ω resp. δ nicht theilbar machen, was voraussetzt, dass x, x'' durch ω resp. durch δ nicht theilbar sei, so ergeben sich ohne weiteres die Gleichungen

$$\left(\frac{\varphi}{\omega}\right) = \left(\frac{\alpha}{\omega}\right), \quad \left(\frac{\Phi}{\delta}\right) = \left(\frac{\alpha\alpha'}{\delta}\right),$$

durch welche der quadratische Charakter für alle durch φ resp. Φ darstellbaren, durch ω resp. δ nicht theilbaren Zahlen als übereinstimmend nachgewiesen wird. Derselbe quadratische Charakter gilt dann aber auch bezüglich der Formen f und $\mathfrak{F}$, welche jenen äquivalent sind.

Die Congruenzen (22) können aber auch dazu verwendet werden, zu zeigen, dass der Form f in Bezug auf eine ungerade Primzahl p, die weder in Ω noch in Δ aufgeht, kein ähnlicher quadratischer Charakter zukommt, dass sie vielmehr in Bezug auf einen solchen Primzahlmodulus sowohl quadratische Reste als Nichtreste darzustellen vermag. Man nehme zu diesem Nachweise $N = p$ an, schreibe also die Congruenzen:

$$\left.\begin{aligned} \varphi &\equiv \alpha x^2 + \alpha'\Omega x'^2 + \alpha''\Omega\Delta x''^2 \\ \Phi &\equiv \alpha'\alpha''\Omega\Delta x^2 + \alpha''\alpha\Delta x'^2 + \alpha\alpha' x''^2 \\ 1 &\equiv \alpha\alpha'\alpha'' \end{aligned}\right\} \pmod{p}.$$

Aus der letzten derselben folgen $\alpha, \alpha', \alpha''$ als prim gegen p, aus der ersten, indem man der Reihe nach x, x', x'' gleich 1, die übrigen Unbestimmten aber jedesmal gleich 0 setzt,

$$\varphi \equiv \alpha, \quad \varphi \equiv \alpha'\Omega, \quad \varphi \equiv \alpha''\Omega\Delta \pmod{p},$$

sodass nichts weiter zu beweisen wäre, wenn diese drei Zahlen verschiedenen quadratischen Charakter besitzen. Im entgegengesetzten Falle aber lässt sich die erste der Con-

gruenzen folgendermassen schreiben:

$$\alpha \cdot \varphi \equiv \mathfrak{x}^2 + \mathfrak{x}'^2 + \mathfrak{x}''^2 \pmod{p}. \tag{33}$$

Sei dann λ irgend welche durch p nicht theilbare Zahl, so kann man auf Grund des Dirichlet'schen Satzes von der arithmetischen Progression eine Primzahl q finden, für welche

$$q \equiv \lambda \pmod{p}, \quad q \equiv 1 \pmod{4}$$

ist, und folglich Zahlen $\mathfrak{x}, \mathfrak{x}'$, welche die Gleichung

$$q = \mathfrak{x}^2 + \mathfrak{x}'^2$$

erfüllen. Wählt man demnach in (33) für $\mathfrak{x}, \mathfrak{x}'$ die eben bestimmten Werthe und setzt $\mathfrak{x}'' = 0$, so kommt

$$\alpha \cdot \varphi \equiv \lambda \pmod{p},$$

wo nun, je nach der Wahl von λ

$$\left(\frac{\varphi}{p}\right) = \left(\frac{\alpha}{p}\right) \text{ oder } = -\left(\frac{\alpha}{p}\right)$$

werden wird. — Was so aus der ersten der Congruenzen für φ erwiesen wurde, das beweist sich in ganz entsprechender Weise aus der zweiten derselben für Φ.

10. Demungeachtet kann man mit Smith einen Gesichtspunkt angeben, von welchem aus sich noch ein weiterer, den in nr. 6 angegebenen ähnlicher Charakter einer Form $f(x, x', x'')$ aufstellen lässt. Wir führen zu diesem Zwecke folgende Definition ein: Ist

$$m = f(x, x', x''), \quad M = \mathfrak{F}(X, X', X'')$$

und sind die Werthe der Unbestimmten, mittels deren diese Darstellungen von m, M durch $f, \mathfrak{F}$ erfolgen, mit einander durch die Gleichung

$$Xx + X'x' + X''x'' = 0 \tag{34}$$

verbunden, so sollen die Darstellungen gleichzeitige und die Zahlen m, M gleichzeitig durch $f, \mathfrak{F}$ dargestellte Zahlen, die gleichzeitigen Darstellungen zudem eigentlich heissen, wenn x, x', x'' sowohl, als auch X, X', X'' keinen von 1 verschiedenen gemeinsamen Theiler haben.

Hiernach werden

$$m = f(x, x', x''), \quad M = \mathfrak{F}(x'y'' - x''y', x''y - xy'', xy' - x'y)$$

gleichzeitige Darstellungen sein. Die erste der Grundformeln

lehrt daher, indem man einmal

$$x = 1, \quad x' = 0, \quad x'' = 0, \quad y = 0, \quad y' = 0, \quad y'' = 1$$

ein andermal

$$x = 1, \quad x' = 0, \quad x'' = 0, \quad y = 0, \quad y' = 1, \quad y'' = 0$$

setzt, dass der erste Coefficient jeder Form f zusammen mit dem zweiten, ebenso auch mit dem dritten Coefficienten ihrer Reciproken $\mathfrak{F}$ ein Paar gleichzeitig und eigentlich dargestellter Zahlen bildet. Allgemeiner zeigt die Art und Weise, wie in der Anmerkung zu nr. 4 des ersten Capitels die erste Grundformel hergeleitet worden ist, dass der erste Coefficient jeder mit f äquivalenten Form mit dem dritten (ebenso auch mit dem zweiten) Coefficienten in der Reciproken derselben gleichzeitig und eigentlich durch $f, \mathfrak{F}$ dargestellt werden. Aber es gilt auch umgekehrt der Satz:

Sind m, M zwei eigentlich und gleichzeitig durch f und $\mathfrak{F}$ dargestellte Zahlen, so kann man eine mit f äquivalente Form angeben, in welcher m der erste, und in deren Reciproker M der (zweite oder) dritte Coefficient ist. Sind nämlich $\alpha_0^0, \alpha_1^0, \alpha_2^0$; $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ die durch die Gleichung

$$\alpha_0^0 \mathsf{A} + \alpha_1^0 \mathsf{A}' + \alpha_2^0 \mathsf{A}'' = 0$$

mit einander verbundenen darstellenden Zahlen, sodass

$$m = f(\alpha_0^0, \alpha_1^0, \alpha_2^0), \qquad M = \mathfrak{F}(\mathsf{A}, \mathsf{A}', \mathsf{A}'')$$

ist, so kann man nach dem Gauss'schen Hilfssatze drei ganze Zahlen $\alpha_0', \alpha_1', \alpha_2'$ so wählen, dass

$$(35) \quad \alpha_1^0\alpha_2' - \alpha_2^0\alpha_1' = \mathsf{A}, \quad \alpha_2^0\alpha_0' - \alpha_0^0\alpha_2' = \mathsf{A}', \quad \alpha_0^0\alpha_1' - \alpha_1^0\alpha_0' = \mathsf{A}''$$

werden, und da letztere Zahlen ein primitives System bilden, lassen sich ferner drei ganze Zahlen $\alpha_0'', \alpha_1'', \alpha_2''$ finden der Art, dass der Modulus der Substitution

$$\begin{aligned} x &= \alpha_0^0 y + \alpha_0' y' + \alpha_0'' y'' \\ x' &= \alpha_1^0 y + \alpha_1' y' + \alpha_1'' y'' \\ x'' &= \alpha_2^0 y + \alpha_2' y' + \alpha_2'' y'' \end{aligned}$$

gleich 1 wird. Durch diese Substitution verwandelt sich aber die Form f in eine äquivalente:

$$a_1 y^2 + a_1' y'^2 + a_1'' y''^2 + 2b_1 y'y'' + 2b_1' y''y + 2b_1'' yy',$$

in welcher

$$a_1 = f(\alpha_0^0, \alpha_1^0, \alpha_2^0) = m, \quad a_1' = f(\alpha_0', \alpha_1', \alpha_2'),$$
$$b_1'' = \alpha_0' f_0^0 + \alpha_1' f_0^1 + \alpha_2' f_0^2,$$

also der dritte Coefficient ihrer Adjungirten gleich

$$\Omega \cdot \mathfrak{F}(\mathsf{A}, \mathsf{A}', \mathsf{A}'') = \Omega \cdot M,$$

mithin der dritte Coefficient ihrer Reciproken gleich M ist.

Indem man m' für a_1', n'' für b_1'' setzt, kann man aus dem Vorigen noch folgenden Schluss ziehen: Sind m, M gleichzeitig und eigentlich durch $f, \mathfrak{F}$ darstellbar, so giebt es eine binäre quadratische Form

$$my^2 + 2n''yy' + m'y'^2$$

mit der Determinante

$$n''^2 - mm' = -\Omega \cdot M \tag{36}$$

durch welche m eigentlich darstellbar ist, während sie ihrerseits eigentlich durch f mittels der Formeln

$$x = \alpha_0^0 y + \alpha_0' y'$$
$$x' = \alpha_1^0 y + \alpha_1' y'$$
$$x'' = \alpha_2^0 y + \alpha_2' y'$$

dargestellt wird.

Und wegen der Reciprocität der Formen $f, \mathfrak{F}$ bezw. der Invarianten Ω, Δ giebt es gleicherweise eine binäre quadratische Form

$$MY^2 + 2N''YY' + M'Y'^2$$

mit der Determinante

$$N''^2 - MM' = -\Delta \cdot m, \tag{37}$$

durch welche M eigentlich darstellbar ist, während sie selbst durch $\mathfrak{F}$ eigentlich dargestellt werden kann.

Hieran fügen wir den Nachweis, dass, wenn von zwei gleichzeitig und eigentlich dargestellten Zahlen m, M die erstere positiv ist, auch die zweite positiv sein muss.

Der ersten Grundformel zufolge besteht die Gleichung

$$m \cdot f(x, x', x'') = (xf_0^0 + x'f_0^1 + x''f_0^2)^2 + \Omega \cdot \mathfrak{F}(X, X', X''),$$

wenn

$$X = \alpha_1{}^0 x'' - \alpha_2{}^0 x', \quad X' = \alpha_2{}^0 x - \alpha_0{}^0 x'', \quad X'' = \alpha_0{}^0 x' - \alpha_1{}^0 x$$

gedacht wird. Nach der zweiten Grundformel erhält man ferner

$$\begin{aligned} & M \cdot \mathfrak{F}(X, X', X'') \\ & = (X\mathfrak{F}^0(\mathsf{A}) + X'\mathfrak{F}^1(\mathsf{A}) + X''\mathfrak{F}^2(\mathsf{A}))^2 \\ & + \varDelta \cdot f(\mathsf{A}'X'' - \mathsf{A}''X', \mathsf{A}''X - \mathsf{A}X'', \mathsf{A}X' - \mathsf{A}'X). \end{aligned}$$

Hier findet sich aber mittels einfacher Rechnung

$$\begin{aligned} \mathsf{A}'X'' - \mathsf{A}''X' &= \alpha_0{}^0(\mathsf{A}x + \mathsf{A}'x' + \mathsf{A}''x'') \\ \mathsf{A}''X - \mathsf{A}X'' &= \alpha_1{}^0(\mathsf{A}x + \mathsf{A}'x' + \mathsf{A}''x'') \\ \mathsf{A}X' - \mathsf{A}'X &= \alpha_2{}^0(\mathsf{A}x + \mathsf{A}'x' + \mathsf{A}''x'') \end{aligned}$$

und somit durch eine Combination der vorstehenden Formeln die folgende Gleichung:

$$(38) \quad \left\{ \begin{aligned} mM \cdot f(x, x', x'') = \; & M \cdot (x f_0^0 + x' f_0^1 + x'' f_0^2)^2 \\ & + \Omega (X\mathfrak{F}^0(\mathsf{A}) + X'\mathfrak{F}^1(\mathsf{A}) + X''\mathfrak{F}^2(\mathsf{A}))^2 \\ & + \Omega \varDelta m \cdot (\mathsf{A}x + \mathsf{A}'x' + \mathsf{A}''x'')^2. \end{aligned} \right.$$

Ist nun m positiv, so würde, falls M negativ wäre, der Ausdruck zur Rechten, so oft $f(x, x', x'')$ eine positive Form ist, also Ω, $\varDelta$ positiv sind, zu einer unbestimmten, so oft $f(x, x', x'')$ aber eine unbestimmte Form, also $\Omega < 0$, $\varDelta > 0$ ist, zu einer bestimmten (negativen) Form, was einen Widerspruch gegen die linke Seite der Gleichung hervorrufen würde; somit muss auch M positiv sein.

11. Nachdem dies festgestellt worden, soll nunmehr der Beweis geführt werden, dass es zwei positive, zu $2\Omega\varDelta$ und auch unter einander prime Zahlen m, M giebt, welche durch f und ihre Reciproke $\mathfrak{F}$ gleichzeitig und eigentlich dargestellt werden können. Nach dem ersten in voriger nr. hervorgehobenen Satze genügt es hierzu, festzustellen, dass es eine mit f äquivalente Form f_1 giebt, in welcher der erste Coefficient und in deren Reciproken $\mathfrak{F}_1$ der dritte Coefficient positiv, zu $2\Omega\varDelta$ und unter einander prim sind; wegen des letzten Satzes reicht es sogar hin, das positive Vorzeichen nur für den erstgenannten Coefficienten festzustellen.

Um sich aber hiervon zu überzeugen, wähle man in den Congruenzen (22) für N den Werth $2\Omega\Delta$, sodass φ eine mit f äquivalente Form bedeutet, für welche und ihre Reciproke Φ die Congruenzen

$$\left.\begin{array}{l}\varphi \equiv \alpha x^2 + \alpha'\Omega x'^2 + \alpha''\Omega\Delta x''^2\\ \Phi \equiv \alpha'\alpha''\Omega\Delta X^2 + \alpha''\alpha\Delta X'^2 + \alpha\alpha' X''^2\\ 1 \equiv \alpha\alpha'\alpha''\end{array}\right\} \pmod{2\Omega\Delta}$$

bestehen, während α, der erste Coefficient von φ, positiv und prim ist gegen $2\Omega\Delta$, auch darf, wenn es beliebt, $\alpha\Delta \equiv 1 \pmod{4}$ vorausgesetzt werden. Versteht man hier unter $\mathfrak{A}$, $\mathfrak{A}', \mathfrak{A}'', \mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ die Coefficienten der Form Φ, so leisten diese den folgenden Congruenzen:

$$\mathfrak{A} \equiv 0,\ \mathfrak{B}' \equiv 0,\ \mathfrak{B}'' \equiv 0 \pmod{\Omega\Delta}$$

Genüge. Demgemäss können $\mathfrak{A}', \mathfrak{A}'', \mathfrak{B}$ keinen gemeinsamen Theiler haben, denn jeder ihnen gemeinsame Primfaktor würde, dem Ausdrucke der Determinante zufolge, auch in der Determinante von Φ also auch in $\Omega\Delta$ und folglich auch in $\mathfrak{A}$, $\mathfrak{B}'$, $\mathfrak{B}''$ aufgehen, die Form Φ also keine primitive sein, was sie doch als reciproke Form sein muss. Da zudem

$$\mathfrak{B} \equiv 0 \pmod{2\Omega\Delta}$$

also gerade ist, muss eine der Zahlen $\mathfrak{A}'$, $\mathfrak{A}''$ ungerade sein und folglich ist die binäre quadratische Form

$$(\mathfrak{A}', \mathfrak{B}, \mathfrak{A}'')$$

eine eigentlich-primitive. Dies vorausgeschickt, bemerke man, dass φ durch eine Substitution

$$x = y,\quad x' = \beta' y' + \beta'' y'',\quad x'' = \gamma' y' + \gamma'' y'',$$

in welcher

$$\beta'\gamma'' - \beta''\gamma' = 1 \tag{39}$$

ist, in eine äquivalente Form f_1 übergeht, deren erster Coefficient der gleiche bleibt, wie in φ, während die Reciproke Φ durch die Substitution

$$X = Y,\quad X' = \gamma'' Y' - \gamma' Y'',\quad X'' = -\beta'' Y' + \beta' Y''$$

in die Reciproke $\mathfrak{F}_1$ übergeht, deren dritter Coefficient demnach durch den Ausdruck

$$\mathfrak{A}'\gamma'^2 + \mathfrak{A}''\beta'^2 - 2\mathfrak{B}\gamma'\beta'$$

bestimmt wird. Da $(\mathfrak{A}', \mathfrak{B}, \mathfrak{A}'')$ eigentlich-primitiv ist, lassen sich die ganzen Zahlen β', γ' so wählen, dass dieser Ausdruck zu $2\Omega\Delta$ und zugleich auch gegen α prim wird*). Man darf sie sogar dabei als relativ prim voraussetzen, sodass es möglich ist, die angenommene Bedingung (39) durch passende Wahl der ganzen Zahlen β'', γ'' zu erfüllen. Die mit f äquivalente Form f_1 ist also genau von der Beschaffenheit, welche nachgewiesen werden sollte.

12. Gesetzt nun, m und M seien zwei solche Zahlen, wie sie als vorhanden soeben nachgewiesen worden sind, so bestehen nach nr. 10 zwei Gleichungen von der Form (36) und (37), aus denen man mit Anwendung des verallgemeinerten Legendre'schen Symbols sogleich die folgenden:

$$\left(\frac{-\Omega M}{m}\right) = 1, \quad \left(\frac{-\Delta m}{M}\right) = 1$$

erschliesst. Aus ihrer Combination und auf Grund des allgemeinen Reciprocitätsgesetzes der quadratischen Reste folgt weiter:

$$\left(\frac{m}{\Omega}\right) \cdot \left(\frac{M}{\Delta}\right) = (-1)^{\frac{\Omega M+1}{2} \cdot \frac{m-1}{2} + \frac{\Delta m+1}{2} \cdot \frac{M-1}{2} + \frac{M-1}{2} \cdot \frac{m-1}{2}}$$

oder, wenn der Exponent von -1 mittels der bekannten für je zwei ungerade Zahlen a, b geltenden Relation

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$$

umgeformt wird, einfacher:

$$\left(\frac{m}{\Omega}\right) \cdot \left(\frac{M}{\Delta}\right) = (-1)^{\frac{\Omega M+1}{2} \cdot \frac{\Delta m+1}{2} + \frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}}.$$

Bezeichnet man demnach mit E die Einheit

$$E = (-1)^{\frac{\Omega M+1}{2} \cdot \frac{\Delta m+1}{2}}, \tag{40}$$

so erhält man für diese die Beziehung:

$$E = (-1)^{\frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}} \cdot \left(\frac{m}{\Omega}\right)\left(\frac{M}{\Delta}\right). \tag{41}$$

Hier ist aber der Werth der rechten Seite theils durch

*) Wenn es beliebt, kann er sogar ausserdem zu einer beliebig gegebenen Zahl prim gemacht werden.

die Ordnung, von welcher der erste Faktor abhängt, theils durch das Geschlecht der Form $f(x, x', x'')$, dem gemäss die Symbole $\left(\frac{m}{\Omega}\right)$, $\left(\frac{M}{\Delta}\right)$ auch durch $\left(\frac{f}{\Omega}\right)$, $\left(\frac{\mathfrak{F}}{\Delta}\right)$ ersetzt werden können, fest bestimmt und für jede zulässige Wahl der Zahlen m, M ein- und derselbe. Man findet demnach, dass für die Form $f(x, x', x'')$ die Einheit E für jedes mögliche Paar von Zahlen m, M von der angegebenen Art einen constanten Werth hat. Letzterer Umstand findet sogar in noch weiterem Umfange statt, als auf dem eben verfolgten Wege gefunden wird. Zum Beweise wähle man in den Congruenzen (22) $N = 4$, wo man ihnen dann, wie einfach zu übersehen, die Gestalt

$$(42) \qquad \left.\begin{cases} \Delta \cdot \varphi \equiv \alpha x^2 + \alpha' x'^2 + \alpha'' x''^2 \\ \Omega \cdot \Phi \equiv \alpha X^2 + \alpha' X'^2 + \alpha'' X''^2 \end{cases}\right\} \pmod{4}$$

geben kann, in welcher $\alpha, \alpha', \alpha''$ wieder drei ganze Zahlen bedeuten, welche der Congruenz

$$(42\text{a}) \qquad \alpha\alpha'\alpha'' \equiv 1 \pmod{4}$$

genügen. Um die Reste zu finden, welche $\Delta \cdot \varphi$, $\Omega \cdot \Phi$ (mod. 4) lassen, wenn man für x, x', x''; X, X', X'' alle primitiven Systeme setzt, welche die Gleichung

$$Xx + X'x' + X''x'' = 0$$

erfüllen, genügt es, diejenigen Restsysteme x, x', x''; X, X', X'' (mod. 4) einzusetzen, für welche die Congruenz

$$Xx + X'x' + X''x'' \equiv 0 \pmod{4}$$

stattfindet. Werden sie zudem so gewählt, dass φ und Φ ungerade werden, so zeigt sich ohne Mühe, dass

$$\frac{\Delta\varphi + 1}{2} \cdot \frac{\Omega\Phi + 1}{2}$$

stets mit einer der drei Zahlen

$$(43) \qquad \frac{(\alpha' + 1)(\alpha'' + 1)}{4}, \quad \frac{(\alpha'' + 1)(\alpha + 1)}{4}, \quad \frac{(\alpha + 1)(\alpha' + 1)}{4}$$

(mod. 2) congruent ist, diese aber sind wegen der Congruenz (42a), aus welcher die andere:

$$(44) \qquad \alpha + \alpha' + \alpha'' + 1 \equiv 0 \pmod{4}$$

hervorgeht, unter einander (mod. 2) congruent. Also ist

$$E = (-1)^{\frac{\Delta m+1}{2} \cdot \frac{\Omega M+1}{2}}$$

für je zwei gleichzeitig durch f, $\mathfrak{F}$ dargestellte *ungerade* Zahlen m, M von gleichbleibendem Werthe.

Der positive oder negative Werth dieser Einheit bezeichnet also in der That einen neuen Charakter der Form $f(x, x', x'')$, den man mit Smith als einen selbständigen (supplementären oder — seiner besonderen Eigenthümlichkeit wegen — simultanen) Charakter den Einzelcharakteren (21) der Form hinzufügen könnte. Dann ist aber zu beachten, dass zwischen ihm und den übrigen Einzelcharakteren der Form die durch die Gleichung (41) ausgesprochene Beziehung stattfindet, der gemäss die Einzelcharaktere zu wählen sind, damit ihnen ein Geschlecht der Ordnung (Ω, Δ) entsprechen kann. Obwohl daher die Anzahl der Werthcombinationen aller Einzelcharaktere durch solche Hinzufügung auf das Doppelte wächst, bleibt dennoch die Anzahl der möglichen Geschlechter unverändert die früher angegebene. Es scheint daher richtiger, E als einen abgeleiteten Charakter zu betrachten, der keiner besonderen Aufzählung bedarf. Aber er giebt Veranlassung, mit Eisenstein die sämmtlichen Geschlechter in die beiden Gruppen zu sondern, bei welchen

$$\text{(a)} \qquad E = 1 \text{ oder } \left(\frac{f}{\Omega}\right) \cdot \left(\frac{\mathfrak{F}}{\Delta}\right) = (-1)^{\frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}}$$

und bei welchen

$$\text{(b)} \qquad E = -1 \text{ oder } \left(\frac{f}{\Omega}\right) \cdot \left(\frac{\mathfrak{F}}{\Delta}\right) = -(-1)^{\frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}}$$

ist. Diese unterscheiden sich nämlich, wie Eisenstein zuerst bemerkt hat, charakteristisch durch ihr Verhalten zum Modulus 8.

In der That, E kann nur -1 sein, wenn $\frac{\Delta m+1}{2} \cdot \frac{\Omega M+1}{2}$ also auch jede der Zahlen (43) ungerade ist; dazu müssen aber $\alpha \equiv \alpha' \equiv \alpha'' \equiv 1 \pmod{4}$ sein und nach der ersten der Congruenzen (42) darf man schreiben

$$\text{(45)} \qquad \Delta \cdot \varphi = (1 + 4\mathfrak{a})x^2 + (1 + 4\mathfrak{a}')x'^2 + (1 + 4\mathfrak{a}'')x''^2 \\ + 4\mathfrak{b}x'x'' + 4\mathfrak{b}'x''x + 4\mathfrak{b}''xx'.$$

Hiernach ist die Determinante von $\Delta \cdot \varphi$ (mod. 8) congruent mit

$$1 + 4(\mathfrak{a} + \mathfrak{a}' + \mathfrak{a}'' - \mathfrak{b}^2 - \mathfrak{b}'^2 - \mathfrak{b}''^2),$$

andererseits ist sie gleich $\Delta^3 \cdot D = \Delta^4 \cdot \Omega^2$ also $\equiv 1$ (mod. 8) und folglich ergiebt sich die Congruenz

$$\mathfrak{a} + \mathfrak{a}' + \mathfrak{a}'' + \mathfrak{b} + \mathfrak{b}' + \mathfrak{b}'' \equiv 0 \text{ (mod. 2)}.$$

Nun müssen, wenn φ ungerade werden soll, die drei Zahlen x, x', x'' entweder sämmtlich ungerade, oder eine von ihnen ungerade, die anderen gerade sein; im letzteren Falle findet man aus (45)

$$\Delta \cdot \varphi \equiv 1 \text{ oder } \Delta \cdot \varphi \equiv 5 \text{ (mod. 8)},$$

im ersteren

$$\Delta \cdot \varphi \equiv 3 + 4(\mathfrak{a} + \mathfrak{a}' + \mathfrak{a}'' + \mathfrak{b} + \mathfrak{b}' + \mathfrak{b}'') \equiv 3 \text{ (mod. 8)}.$$

Hieraus aber folgt der Satz: **Durch eine Form aus der zweiten der Geschlechtsgruppen sind ungerade Zahlen darstellbar, welche einer beliebigen der Zahlen Δ, 3Δ, 5Δ, aber keine, welche 7Δ (mod. 8) congruent sind.**

Soll dagegen $E = +1$ sein, so muss $\frac{\Delta m + 1}{2} \cdot \frac{\Omega M + 1}{2}$ also jede der Zahlen (43) gerade sein, was erfordert, dass mindestens zwei der Zahlen $\alpha, \alpha', \alpha''$, z. B. α, α' congruent 3 und dann wegen (44) die dritte derselben, α'' congruent 1 (mod. 4) sei. Man darf dann also schreiben:

$$(46) \qquad \Delta \cdot \varphi = (3 + 4\mathfrak{a})x^2 + (3 + 4\mathfrak{a}')x'^2 + (1 + 4\mathfrak{a}'')x''^2 + 4\mathfrak{b}x'x'' + 4\mathfrak{b}'x''x + 4\mathfrak{b}''xx'$$

und erschliesst nun wieder wie vorher die Congruenz

$$\mathfrak{a} + \mathfrak{a}' + \mathfrak{a}'' + \mathfrak{b} + \mathfrak{b}' + \mathfrak{b}'' \equiv 0 \text{ (mod. 2)}.$$

Wählt man also x, x', x'' wieder auf alle mögliche Weise so, dass φ ungerade wird, so sieht man leicht ein, dass $\Delta \cdot \varphi$ jeden der Reste 1, 3, 5, 7 (mod. 8) lassen kann, und gelangt so zu dem Satze: **Durch eine Form aus der ersten Geschlechtsgruppe können Zahlen von jeder der Linearformen $8n + 1, 3, 5, 7$ dargestellt werden.**

Drittes Capitel.

Von der Darstellung durch eine gegebene Form.

1. Im vorigen Capitel ist eine Reihe von Sätzen über die Darstellung von Zahlen oder von binären quadratischen Formen durch ternäre entwickelt, die zwar an sich hohe Bedeutung besitzen und auch häufig, insofern sie Bedingungen für die Darstellbarkeit zum Ausdruck bringen, erkennen lassen, wenn etwa eine gegebene Zahl durch eine gegebene Form nicht dargestellt werden kann. Die Aufgabe aber, diese Entscheidung für jeden Fall zu treffen und alle etwa vorhandenen Darstellungen einer gegebenen Zahl sowie einer gegebenen binären durch eine gegebene ternäre quadratische Form aufzustellen, bleibt noch zu lösen. Im gegenwärtigen Capitel wird die Lösung dieser Aufgabe auseinandergesetzt, wie sie Gauss gelehrt hat*).

1) Beginnen wir mit der an die Betrachtungen des vorigen Capitels unmittelbar sich anschliessenden Bemerkung, dass, wenn eine binäre quadratische Form

$$(1) \qquad \varphi = my^2 + 2n''yy' + m'y'^2$$

mit der Determinante

$$(2) \qquad D = n''^2 - mm' \text{ **)}$$

durch die ternäre quadratische Form $f(x, x', x'')$ darstellbar ist, indem man

$$(3) \qquad \begin{cases} x = \alpha_0{}^0 y + \alpha_0{}' y' \\ x' = \alpha_1{}^0 y + \alpha_1{}' y' \\ x'' = \alpha_2{}^0 y + \alpha_2{}' y' \end{cases}$$

setzt, sich die Beziehungen

$$(4) \qquad \begin{cases} m = f(\alpha_0{}^0, \alpha_1{}^0, \alpha_2{}^0), \quad n'' = \alpha_0{}' f_0{}^0 + \alpha_1{}' f_0{}^1 + \alpha_2{}' f_0{}^2, \\ m' = f(\alpha_0{}', \alpha_1{}', \alpha_2{}') \end{cases}$$

---

*) Disquisitiones Arithmeticae, art. 278 bis 285.

**) Unter D ist fortan nicht mehr, wie bisher, die Determinante der ternären Form zu verstehen, welche überhaupt nicht mehr durch einen besonderen Buchstaben auszudrücken ist, da sie mittels der beiden Invarianten Ω, Δ ausgedrückt werden kann.

und folglich nach der ersten Grundformel auch die folgende:

(5) $D = -\Omega \cdot \mathfrak{F}(\alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1',\ \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2',\ \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0')$

ergeben. Hieraus folgt: Damit eine binäre quadratische Form durch eine ternäre von der Ordnung (Ω, Δ) darstellbar ist, muss ihre Determinante D durch Ω theilbar sein, und wenn man

(6) $$D = -\Omega \cdot M''$$

setzt, so ist nach der Gleichung

(7) $M'' = \mathfrak{F}(\alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1',\ \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2',\ \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0')$

jeder Darstellung der binären Form durch die ternäre eine Darstellung von M'' durch die Reciproke der ternären Form zugeordnet; auch wird letztere Darstellung eine eigentliche sein, so oft es die erstere ist.

2) Man kann aber auch umgekehrt zeigen, dass jede eigentliche Darstellung von M'' durch die Form $\mathfrak{F}$ einer eigentlichen Darstellung einer binären Form mit der Determinante $D = -\Omega \cdot M''$ durch die Form f zugeordnet ist. In der That sei

$$M'' = \mathfrak{F}(\mathsf{A}, \mathsf{A}', \mathsf{A}''),$$

wo die darstellenden Zahlen $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ keinen von 1 verschiedenen gemeinsamen Theiler haben. Wählt man dann nach dem Gauss'schen Hilfssatze die ganzen Zahlen $\alpha_0{}^0, \alpha_1{}^0, \alpha_2{}^0, \alpha_0', \alpha_1', \alpha_2'$ der Art, dass

$$\alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1' = \mathsf{A},\quad \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2' = \mathsf{A}',\quad \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0' = \mathsf{A}''$$

ist, so bestimmen die Formeln (3) eine eigentliche Darstellung einer quadratischen Form (m, n'', m') mit den durch (4) definirten Coefficienten und mit der Determinante D durch die Form $f(x, x', x'')$, eine Darstellung, welcher die Darstellung $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ von M'' durch $\mathfrak{F}$ zugeordnet ist.

3) Aequivalente binäre Formen mit der Determinante $D = -M''\Omega$ sind immer gleichzeitig durch die Form $f(x, x', x'')$ (eigentlich) darstellbar oder gleichzeitig nicht darstellbar*), und liefern im ersteren

*) Dieser Theil des Satzes bleibt, wie leicht zu übersehen, auch bei uneigentlicher Aequivalenz von φ und φ' bestehen.

Falle dieselben zugeordneten Darstellungen von M'' durch die Form $\mathfrak{F}$. Denn, ist φ' äquivalent mit φ, so besteht für eine Substitution

(8) $$y = \alpha z + \beta z', \quad y' = \gamma z + \delta z',$$

in welcher $\alpha\delta - \beta\gamma = 1$ ist, die Gleichung

$$\varphi'(z, z') = \varphi(y, y').$$

Wenn dann φ durch $f(x, x', x'')$ (eigentlich) darstellbar ist mittels der Formeln (3), sodass

(9) $$f(\alpha_0{}^0 y + \alpha_0' y', \alpha_1{}^0 y + \alpha_1' y', \alpha_2{}^0 y + \alpha_2' y') = \varphi(y, y')$$

ist, so ist auch

(10) $$f(\beta_0{}^0 z + \beta_0' z', \beta_1{}^0 z + \beta_1' z', \beta_2{}^0 z + \beta_2' z') = \varphi'(z, z')$$

d. h. φ' ist darstellbar durch $f(x, x', x'')$ mittels der Formeln

(11) $$\begin{cases} x = \beta_0{}^0 z + \beta_0' z' = (\alpha_0{}^0\alpha + \alpha_0'\gamma) z + (\alpha_0{}^0\beta + \alpha_0'\delta) z' \\ x' = \beta_1{}^0 z + \beta_1' z' = (\alpha_1{}^0\alpha + \alpha_1'\gamma) z + (\alpha_1{}^0\beta + \alpha_1'\delta) z' \\ x'' = \beta_2{}^0 z + \beta_2' z' = (\alpha_2{}^0\alpha + \alpha_2'\gamma) z + (\alpha_2{}^0\beta + \alpha_2'\delta) z' \end{cases}$$

und man findet sogleich

$$\beta_1{}^0\beta_2' - \beta_2{}^0\beta_1' = \alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1'$$
$$\beta_2{}^0\beta_0' - \beta_0{}^0\beta_2' = \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2'$$
$$\beta_0{}^0\beta_1' - \beta_1{}^0\beta_0' = \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0'.$$

4) Verschiedenen Transformationen von φ in φ' entsprechen auch verschiedene, der Darstellung von φ zugehörige Darstellungen von φ'. Denn, da die Zahlen

$$\alpha_1{}^0\alpha_2' - \alpha_2{}^0\alpha_1', \quad \alpha_2{}^0\alpha_0' - \alpha_0{}^0\alpha_2', \quad \alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0'$$

ohne gemeinsamen Theiler sind, können sie nicht sämmtlich Null sein; sei also etwa $\alpha_0{}^0\alpha_1' - \alpha_1{}^0\alpha_0'$ von Null verschieden. Dann ersieht man sogleich, dass aus den Werthen von

$$\alpha_0{}^0\alpha + \alpha_0'\gamma, \quad \alpha_1{}^0\alpha + \alpha_1'\gamma$$

die Zahlen α, γ, aus den Werthen von

$$\alpha_0{}^0\beta + \alpha_0'\delta, \quad \alpha_1{}^0\beta + \alpha_1'\delta$$

die Zahlen β, δ eindeutig bestimmt sind; verschiedenen Systemen $\alpha, \beta, \gamma, \delta$ kann also nicht dieselbe Darstellung (11) entsprechen.

Legt man den Zahlen α, β, γ, δ alle Werthe bei, welche

die Gleichung $\alpha\delta - \beta\gamma = 1$ erfüllen, so erhält man auch diejenigen τ Substitutionen (8), welche φ in sich selbst verwandeln. Indem man also φ' mit φ identificirt, folgt sogleich aus dem eben Gesagten, dass τ verschiedenen Darstellungen von φ durch f immer ein und dieselbe Darstellung von M'' durch $\mathfrak{F}$ zugeordnet ist. Hierbei ist τ unendlich, wenn $D > 0$ ist, dagegen eine aus der Theorie der binären quadratischen Formen her bekannte endliche Zahl, wenn $D < 0$ ist.

5) Nicht äquivalente, durch die Form $f(x, x', x'')$ eigentlich darstellbare binäre Formen mit der Determinante $D = -\Omega M''$ liefern verschiedene zugeordnete Darstellungen von M'' durch $\mathfrak{F}$. In der That, wären φ und φ' zwei nicht äquivalente binäre Formen mit der Determinante D, von denen die erste mittels der Gleichung (9), die zweite mittels der Gleichung (10) durch $f(x, x', x'')$ eigentlich darstellbar ist, während diesen Darstellungen dieselbe eigentliche Darstellung $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ von M'' durch $\mathfrak{F}$ zugeordnet ist, so beständen sowohl die Gleichungen

$$\alpha_1{}^0\alpha_2{}' - \alpha_2{}^0\alpha_1{}' = \mathsf{A},\quad \alpha_2{}^0\alpha_0{}' - \alpha_0{}^0\alpha_2{}' = \mathsf{A}',\quad \alpha_0{}^0\alpha_1{}' - \alpha_1{}^0\alpha_0{}' = \mathsf{A}''$$

als auch die Gleichungen

$$\beta_1{}^0\beta_2{}' - \beta_2{}^0\beta_1{}' = \mathsf{A},\quad \beta_2{}^0\beta_0{}' - \beta_0{}^0\beta_2{}' = \mathsf{A}',\quad \beta_0{}^0\beta_1{}' - \beta_1{}^0\beta_0{}' = \mathsf{A}''.$$

Nach nr. 7 des vorigen Capitels müssten daher

$$\begin{aligned} \beta_0{}^0 &= \alpha\alpha_0{}^0 + \gamma\alpha_0{}' \qquad & \beta_0{}' &= \beta\alpha_0{}^0 + \delta\alpha_0{}' \\ \beta_1{}^0 &= \alpha\alpha_1{}^0 + \gamma\alpha_1{}' \qquad & \beta_1{}' &= \beta\alpha_1{}^0 + \delta\alpha_1{}' \\ \beta_2{}^0 &= \alpha\alpha_2{}^0 + \gamma\alpha_2{}' \qquad & \beta_2{}' &= \beta\alpha_2{}^0 + \delta\alpha_2{}' \end{aligned}$$

sein, während $\alpha\delta - \beta\gamma = 1$ ist, was nichts anderes besagt, als dass φ in φ' durch eine Substitution (8) transformirbar, ihr also äquivalent wäre, gegen die Voraussetzung.

2. Aus diesen fünf festgestellten Umständen ist offenbar nun Folgendes zu erschliessen:

Wegen 2) werden nothwendig sämmtliche eigentliche Darstellungen von M'' durch die Form $\mathfrak{F}$ erhalten, wenn man die eigentlichen Darstellungen aller binären quadratischen Formen mit der Determinante $D = -\Omega M''$ durch die Form f aufsucht. Es genügt aber nach 3), dies für alle nicht-äquivalenten

Formen $\varphi, \varphi', \varphi'', \ldots$ mit dieser Determinante zu thun. Nach 1) liefert wirklich jede solche Darstellung einer dieser Formen eine der gesuchten Darstellungen von M'' und nach 5) sind jedenfalls diejenigen so ermittelten Darstellungen von M'', welche verschiedenen der Formen $\varphi, \varphi', \varphi'', \ldots$ entsprechen, von einander verschieden. Was aber diejenigen Darstellungen von M'' betrifft, welche Darstellungen ein und derselben der Formen $\varphi, \varphi', \varphi'', \ldots$ zugeordnet sind, so werden nach 4) die letztern sich in Complexe von je τ Darstellungen vertheilen der Art, dass jedem dieser Complexe nur eine einzige aber wegen 5) auch eine eigene, von den andern verschiedene Darstellung von M'' zugeordnet ist.

Die entwickelten Betrachtungen lehren aber weiter, dass die Aufgabe: alle eigentlichen Darstellungen einer gegebenen *Zahl* durch eine gegebene ternäre quadratische Form zu finden, auf die andere zurückkommt: alle eigentlichen Darstellungen einer gegebenen *binären* quadratischen *Form* durch eine gegebene ternäre zu ermitteln. In der That, nach dem eben Gesagten findet man die eigentlichen Darstellungen einer gegebenen Zahl M'' durch die Reciproke einer ternären Form der Ordnung (Ω, Δ) aus den eigentlichen Darstellungen binärer Formen mit der Determinante $-\Omega M''$ durch die ternäre Form selbst; aber jede gegebene ternäre Form einer beliebigen Ordnung (Ω, Δ) kann als Reciproke einer solchen angesehen werden, deren Invarianten bis auf das Vorzeichen Δ, Ω sind und damit leuchtet die Richtigkeit des ausgesprochenen Satzes unmittelbar ein.

3. Man hat demnach fortan nur noch zu handeln von der eigentlichen Darstellung einer gegebenen binären quadratischen Form

$$\varphi = my^2 + 2n''yy' + m'y'^2$$

durch eine gegebene ternäre Form $f(x, x', x'')$, deren Ordnung wieder durch die Invarianten Ω, Δ bestimmt angenommen werden mag. Vor allem müssen die Bedingungen festgestellt werden, unter denen solche Darstellung allein möglich ist.

Nach nr. 1 weiss man bereits eine derselben: die Determinante D der binären Form muss durch Ω theilbar sein; wir setzen also

(12) $$D = -\Omega \cdot M''$$

Für die Anwendungen der Darstellungslehre, die wir zu machen gedenken, wird es genügen, wenn wir fortan uns auf die Voraussetzung beschränken, dass M'' prim sei zu $2\Omega\Delta$. Ist aber φ mittels der Formeln (3) durch $f(x, x', x'')$ darstellbar, so folgt die Gleichung

(13) $$M'' = \mathfrak{F}(\alpha_1^0\alpha_2' - \alpha_2^0\alpha_1',\ \alpha_2^0\alpha_0' - \alpha_0^0\alpha_2',\ \alpha_0^0\alpha_1' - \alpha_1^0\alpha_0')$$

d. h. M'' ist durch die Reciproke $\mathfrak{F}$ von f darstellbar und folglich muss *zweitens* für jede in Δ aufgehende Primzahl δ die Bedingung

(14) $$\left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right)$$

erfüllt sein. Wenn f eine bestimmte (positive) Form, also $\Omega > 0$ ist, kann offenbar auch φ nur eine positive binäre Form sein, in ihrer Determinante $D = -\Omega M''$ muss also $M'' > 0$ sein. Ist dagegen f eine unbestimmte Form, also $\Omega < 0$, so muss φ eine bestimmte oder unbestimmte Form sein, je nachdem $M'' < 0$ oder $M'' > 0$ ist, und im ersteren Fall eine negative Form, denn sonst wären m, M'' zwei eigentlich und gleichzeitig durch f und $\mathfrak{F}$ dargestellte Zahlen und $m > 0$, $M'' < 0$, gegen nr. 10 vorigen Capitels. —

Da die Darstellung der Form φ als eine eigentliche vorausgesetzt wird, so lassen sich die ganzen Zahlen α_0'', α_1'', α_2'' so angeben, dass die Determinante

(15) $$\begin{vmatrix} \alpha_0^0 & \alpha_0' & \alpha_0'' \\ \alpha_1^0 & \alpha_1' & \alpha_1'' \\ \alpha_2^0 & \alpha_2' & \alpha_2'' \end{vmatrix} = 1$$

ist. Nimmt man die Zahlen $A_0^0, A_0', \ldots$ in ihrer früheren Bedeutung (Cap. 1, (30)), so erhält man mit Rücksicht auf die Gleichung (13), die dann einfacher

$$M'' = \mathfrak{F}(A_0'', A_1'', A_2'')$$

lautet, aus der zweiten Grundformel folgende Congruenz

$$(16)\quad \begin{cases} 0 \equiv (x\mathfrak{F}^0(\mathsf{A}'') + x'\mathfrak{F}^1(\mathsf{A}'') + x''\mathfrak{F}^2(\mathsf{A}''))^2 \\ \quad + \varDelta \cdot f(x'\mathsf{A}_2'' - x''\mathsf{A}_1'',\ x''\mathsf{A}_0'' - x\mathsf{A}_2'',\ x\mathsf{A}_1'' - x'\mathsf{A}_0'') \\ \qquad\qquad (\text{mod. } M''). \end{cases}$$

Setzt man hier zur Abkürzung

$$(17)\quad x\alpha_0^0 + x'\alpha_1^0 + x''\alpha_2^0 = u, \quad x\alpha_0' + x'\alpha_1' + x''\alpha_2' = u',$$

so findet man sogleich

$$\begin{aligned} x'\mathsf{A}_2'' - x''\mathsf{A}_1'' &= \alpha_0^0 u' - \alpha_0' u \\ x''\mathsf{A}_0'' - x\mathsf{A}_2'' &= \alpha_1^0 u' - \alpha_1' u \\ x\mathsf{A}_1'' - x'\mathsf{A}_0'' &= \alpha_2^0 u' - \alpha_2' u \end{aligned}$$

und wegen der Darstellbarkeit der Form φ durch f mittels der Formeln (3)

$$f(\alpha_0^0 u' - \alpha_0' u,\ \alpha_1^0 u' - \alpha_1' u,\ \alpha_2^0 u' - \alpha_2' u) \\ = m u'^2 - 2n'' u' u + m' u^2.$$

Hierdurch nimmt die Congruenz (16) die neue Gestalt an:

$$(x\mathfrak{F}^0(\mathsf{A}'') + x'\mathfrak{F}^1(\mathsf{A}'') + x''\mathfrak{F}^2(\mathsf{A}''))^2 \\ + \varDelta(m u'^2 - 2n'' u' u + m' u^2) \equiv 0 \ (\text{mod. } M'')$$

und ergiebt, wenn man einmal x, x', x'' gleich $\mathsf{A}_0', \mathsf{A}_1', \mathsf{A}_2'$, ein zweites Mal gleich $\mathsf{A}_0^0, \mathsf{A}_1^0, \mathsf{A}_2^0$, ein drittes Mal gleich

$$\mathsf{A}_0' + \mathsf{A}_0^0,\ \mathsf{A}_1' + \mathsf{A}_1^0,\ \mathsf{A}_2' + \mathsf{A}_2^0$$

wählt, die folgenden drei Congruenzen:

$$(18)\quad N^2 + \varDelta m \equiv 0, \quad NN' - \varDelta n'' \equiv 0, \quad N'^2 + \varDelta m' \equiv 0 \\ (\text{mod. } M''),$$

in denen

$$(19)\quad \begin{cases} N = \mathsf{A}_0'\mathfrak{F}^0(\mathsf{A}'') + \mathsf{A}_1'\mathfrak{F}^1(\mathsf{A}'') + \mathsf{A}_2'\mathfrak{F}^2(\mathsf{A}'') \\ N' = \mathsf{A}_0^0\mathfrak{F}^0(\mathsf{A}'') + \mathsf{A}_1^0\mathfrak{F}^1(\mathsf{A}'') + \mathsf{A}_2^0\mathfrak{F}^2(\mathsf{A}'') \end{cases}$$

gesetzt ist, drei Congruenzen, welche auch in die einzige:

$$(20)\quad (Ny - N'y')^2 + \varDelta(my^2 + 2n'' y y' + m' y'^2) \equiv 0 \\ (\text{mod. } M'')$$

zusammengefasst werden können. Damit also die binäre quadratische Form φ durch f eigentlich darstellbar sei, ist erforderlich, dass die Congruenz (20) auflösbar oder — wie Gauss es ausdrückt — dass

$$-\varDelta(my^2 + 2n'' y y' + m' y'^2)$$

quadratischer Rest ist (mod. M'').

Jede vorhandene eigentliche Darstellung der Form φ durch f liefert mittels der Formeln (19) eine Lösung der Congruenz (20) oder der gleichbedeutenden Congruenzen (18); sie liefert aber nicht nur eine, sondern unendlich viel solche Lösungen. In der That, ob auch die Darstellung (3) gegeben ist, so bleiben doch die Zahlen α_0'', α_1'', α_2'' noch auf mannigfaltige Weise so wählbar, dass die Gleichung (15) erfüllt wird, und aus einer Lösung dieser letztern ergeben sich alle andern mittels der Formeln:

$$(21)\qquad \beta_0'' = \alpha_0'' - h'\mathsf{A}_2'' + h''\mathsf{A}_1'', \quad \beta_1'' = \alpha_1'' - h''\mathsf{A}_0'' + h\mathsf{A}_2'', \quad \beta_2'' = \alpha_2'' - h\mathsf{A}_1'' + h'\mathsf{A}_0'';$$

ersetzt man aber α_0'', α_1'', α_2'' durch diese Werthe, so gehen A_0^0, A_1^0, A_2^0, A_0', A_1', A_2' resp. über in

$$\begin{array}{l}
\mathsf{A}_0^0 + \mathsf{A}_0''(h\alpha_0' + h'\alpha_1' + h''\alpha_2') \\
\mathsf{A}_1^0 + \mathsf{A}_1''(h\alpha_0' + h'\alpha_1' + h''\alpha_2') \\
\mathsf{A}_2^0 + \mathsf{A}_2''(h\alpha_0' + h'\alpha_1' + h''\alpha_2') \\
\mathsf{A}_0' - \mathsf{A}_0''(h\alpha_0^0 + h'\alpha_1^0 + h''\alpha_2^0) \\
\mathsf{A}_1' - \mathsf{A}_1''(h\alpha_0^0 + h'\alpha_1^0 + h''\alpha_2^0) \\
\mathsf{A}_2' - \mathsf{A}_2''(h\alpha_0^0 + h'\alpha_1^0 + h''\alpha_2^0)
\end{array}$$

also N und N' in

$$(22)\qquad \begin{cases} N_1 = N - (h\alpha_0^0 + h'\alpha_1^0 + h''\alpha_2^0)M'' \\ N_1' = N' + (h\alpha_0' + h'\alpha_1' + h''\alpha_2')M'' \end{cases}$$

d. i. in eine (mod. M'') congruente Lösung der Congruenzen (18) über. Das an Stelle von α_0'', α_1'', α_2'' gesetzte System β_0'', β_1'', β_2'' kann aber auch so gewählt werden, dass ihm eine beliebig gegebene mit N, N' (mod. M'') congruente Lösung dieser Congruenzen entspricht. Denn man kann, wenn

$$N_1 = N - rM'', \quad N_1' = N' + sM''$$

ist, wo r, s beliebig gegebene Zahlen bedeuten, die ganzen Zahlen h, h', h'' auf unendlich mannigfaltige Weise so bestimmen, dass

$$\begin{array}{l}
h\alpha_0^0 + h'\alpha_1^0 + h''\alpha_2^0 = r \\
h\alpha_0' + h'\alpha_1' + h''\alpha_2' = s
\end{array}$$

ist, und jeder solchen Bestimmung entspricht ein System von Zahlen β_0'', β_1'', β_2'' von der verlangten Beschaffenheit.

Nennt man folglich alle unter einander congruenten Lösungen der Congruenzen (18) eine einzige Wurzel derselben, so ist aus dem Bemerkten ersichtlich, dass jeder eigentlichen Darstellung der Form φ durch f eine ganz bestimmte Wurzel jener Congruenzen entspricht oder dass — in Gaussscher Ausdrucksweise — jede solche Darstellung zu einer bestimmten *Wurzel* der Congruenz (20) oder zu einem bestimmten *Werthe* des Ausdrucks

$$\sqrt{-\Delta(my^2 + 2n''yy' + m'y'^2)} \pmod{M''}$$

gehört. Ist zudem N, N' ein ganz nach Belieben unter allen congruenten Lösungen gewählter Repräsentant dieser Wurzel, so können die ganzen Zahlen α_0'', α_1'', α_2'' so gewählt werden, dass, während sie der Gleichung (15) genügen, ihnen gerade diese Lösung correspondirt. Durch die Substitution

$$\begin{aligned} x &= \alpha_0^0 y + \alpha_0' y' + \alpha_0'' y'' \\ x' &= \alpha_1^0 y + \alpha_1' y' + \alpha_1'' y'' \\ x'' &= \alpha_2^0 y + \alpha_2' y' + \alpha_2'' y'' \end{aligned}$$

geht dann aber offenbar die Form $f(x, x', x'')$ in eine äquivalente Form

$$my^2 + m'y'^2 + m''y''^2 + 2ny'y'' + 2n'y''y + 2n''yy'$$

mit der Reciproken

$$My^2 + M'y'^2 + M''y''^2 + 2Ny'y'' + 2N'y''y + 2N''yy'$$

über. Mit andern Worten:

Ist eine Form φ eigentlich durch f darstellbar und (N, N') ein beliebig gewählter Repräsentant der Wurzel (mod. M''), zu welcher diese Darstellung gehört, so giebt es eine mit f äquivalente Form, von welcher die Form φ einen Bestandtheil ausmacht, und in deren Reciproker der 3te, 4te, 5te Coefficient resp. M'', N und N' sind.

Hiernach erkennt man leicht, dass die Form φ *primitiv* sein muss, um durch eine Form f der Ordnung (Ω, Δ) eigentlich darstellbar zu sein. Denn zwischen den Coefficienten der beiden reciproken Formen bestehen die folgenden Beziehungen:

$$\Delta \cdot m = M'M'' - N^2, \quad \Delta \cdot m' = M''M - N'^2,$$
$$\Delta \cdot m'' = MM' - N''^2, \quad \Delta \cdot n'' = NN' - M''N'',$$

aus denen sich die weitere:

$$\Delta(Mm + 2N''n'' + M'm') = \Omega\Delta^2 + M'' \cdot \Delta m''$$

ergiebt, eine Formel, welcher jede der beiden Gestalten:

$$Mm + 2N''n'' + M'm' = \Omega\Delta + M''m''$$

und

$$\Omega(Mm + 2N''n'' + M'm') = \Omega^2\Delta - m''(n''^2 - mm')$$

gegeben werden kann. Die letztere lässt erkennen, dass jeder gemeinsame Theiler von m, n'', m', welcher auch in der Determinante $-\Omega M''$ der binären Form aufgeht, in $\Omega^2\Delta$, folglich, da M'' zu $2\Omega\Delta$ prim vorausgesetzt ist, in Ω aufgehen, mithin zu M'' prim sein muss. Daher zeigt die erstere Gestalt der Formel, dass er auch aufgeht in m''. Ferner aber bestehen die Beziehungen:

$$n'n'' - mn = \Omega N, \quad n''n - m'n' = \Omega N'$$

und aus ihnen folgen die andern:

$$M''n = -Nm' - N'n'', \quad M''n' = -Nn'' - N'm,$$

welche lehren, dass der gemeinsame Theiler von m, n'', m' auch in n und n' aufgehen muss. Wäre er also von 1 verschieden, so wäre die Form, von welcher φ ein Bestandtheil ist, nicht primitiv, obwohl sie der primitiven Form f äquivalent ist.

4. Die Congruenzbedingung (20), die zur eigentlichen Darstellbarkeit der Form φ durch f erforderlich ist, kann durch eine andere Bedingung ersetzt werden, welche ihr völlig gleichbedeutend ist. Zur Erfüllbarkeit der Congruenz (20) ist nämlich nothwendig und hinreichend, dass in Bezug auf jede der (ungeraden) Primzahlen p, aus welchen M'' sich zusammensetzt, der quadratische Charakter von $-\Delta$ mit demjenigen der binären Form φ übereinstimme. Dies ist in der That zunächst erforderlich. Denn, soll die Congruenz (20) oder die drei gleichbedeutenden Congruenzen (18) (mod. M'') stattfinden, so muss auch

$$N^2 + \Delta m \equiv 0, \; NN' - \Delta n'' \equiv 0, \; N'^2 + \Delta m' \equiv 0 \pmod{p}$$

sein; eine der Zahlen m und m' ist aber sicher durch p nicht theilbar, da sonst wegen $n''^2 - mm' = -\Omega M''$ auch n'' durch p theilbar wäre, während doch φ als eine primitive Form vorausgesetzt werden muss. Ist also etwa m nicht theilbar durch p, so ergiebt sich aus der ersten der voraufgehenden Congruenzen

$$\left(\frac{-\Delta m}{p}\right) = 1 \text{ d. h. } \left(\frac{-\Delta}{p}\right) = \left(\frac{m}{p}\right),$$

oder auch

$$(23) \qquad \left(\frac{-\Delta}{p}\right) = \left(\frac{\varphi}{p}\right).$$

Das Stattfinden dieser Gleichung für jede der in M'' aufgehenden Primzahlen p ist aber auch ausreichend für die Erfüllbarkeit der Congruenz (20). Denn wenn sie für eine dieser Primzahlen p stattfindet, so ist zuerst, wenn von den beiden Coefficienten m, m' etwa m der nicht durch p theilbare ist,

$$\left(\frac{m}{p}\right) = \left(\frac{\varphi}{p}\right) = \left(\frac{-\Delta}{p}\right)$$

also ist, wenn p^α die in M'' aufgehende Potenz dieses Primfaktors bezeichnet, die Congruenz

$$N^2 + \Delta m \equiv 0 \pmod{p^\alpha}$$

auflösbar; ist N eine Lösung derselben, so kann man eine Zahl N' finden, für welche

$$mN' + n''N \equiv 0 \pmod{p^\alpha},$$

und dann folgen die Congruenzen

$$mNN' + n''N^2 \equiv mNN' - \Delta mn'' \equiv 0$$

also

$$NN' - \Delta n'' \equiv 0,$$

und

$$mN'^2 + n''NN' \equiv mN'^2 + n''^2\Delta \equiv mN'^2 + mm'\Delta \equiv 0$$

also

$$N'^2 + \Delta m' \equiv 0 \pmod{p^\alpha}.$$

Die Congruenzen (18) sind also (mod. p^α) erfüllt. Da dies aber für jede der Primzahlpotenzen gilt, wenn (23) für jede der Primzahlen stattfindet, aus denen M'' sich zusammensetzt, werden zwei Zahlen, welche nach den einzelnen derselben congruent den entsprechenden Lösungen N, N' gewählt werden,

auch eine Lösung der Congruenzen (18) (mod. M'') liefern, die Congruenz (20) also auflösbar sein.

Hieraus folgt u. A., was für später bemerkt werden muss, dass für alle binären Formen (m, n'', m') ein- und desselben Geschlechts die Zahlen Δ, für welche die Congruenz (20) stattfinden kann, dieselben bleiben. Auch leuchtet ein, dass in dem Falle, wo die Form $(-m, -n'', -m')$ zum Hauptgeschlecht ihrer Determinante gehört, $\Delta = +1$ eine zulässige Zahl ist, anders ausgedrückt: dass alsdann die Congruenz

$$(24)\quad (Ny - N'y')^2 + my^2 + 2n''y'y + m'y'^2 \equiv 0 \pmod{M''}$$

auflösbar ist.

Unter der Voraussetzung, dass die Congruenz (20) möglich ist, kann leicht die Anzahl ihrer Wurzeln bestimmt werden. Jede Lösung derselben ist auch — die gleichen Bezeichnungen gesetzt, wie zuvor — eine Lösung der folgenden:

$$(25)\quad N^2 + \Delta m \equiv 0,\; NN' - \Delta n'' \equiv 0,\; N'^2 + \Delta m' \equiv 0 \pmod{p^\alpha}.$$

Ist nun N_1, N_1' irgend eine weitere Lösung der letzteren, so müsste

$$(26)\quad N_1^2 + \Delta m \equiv 0,\; N_1 N_1' - \Delta n'' \equiv 0,\; N_1'^2 + \Delta m' \equiv 0$$

also

$$(N_1 - N)\cdot(N_1 + N) \equiv 0 \pmod{p^\alpha}$$

sein; beide Faktoren zur Linken können aber nicht durch p theilbar sein, weil es sonst auch N sein müsste gegen die erste der Congruenzen (25), wenn man, was erlaubt ist, m als nicht durch p theilbar voraussetzt. Man schliesst also

$$N_1 \equiv \pm N \pmod{p^\alpha}$$

und nun aus der Vergleichung der zweiten der Congruenzen (25) und (26) entsprechend

$$N_1' \equiv \pm N' \pmod{p^\alpha}$$

d. i. also entweder

$$N_1 \equiv N,\quad N_1' \equiv N'$$

oder

$$\left.\begin{array}{ll} N_1 \equiv N, & N_1' \equiv N' \\ N_1 \equiv -N, & N_1' \equiv -N' \end{array}\right\} \pmod{p^\alpha}.$$

Dass jedes dieser Werthsysteme auch umgekehrt eine Lösung der Congruenzen (25) ausmacht, bedarf keines Nachweises.

Da aber die Congruenz

$$N \equiv -N$$

nicht zulässig ist, haben also die Congruenzen (25) genau zwei incongruente Lösungen oder sie haben zwei Wurzeln. Dies gilt für jede der in M'' aufgehenden Primzahlpotenzen. Aber für jede Combination von Wurzeln der nach diesen einzelnen Primzahlpotenzmoduln genommenen Congruenzen wird durch das oben angedeutete Verfahren eine Wurzel der Congruenzen (18), und für verschiedene Combinationen nothwendig auch verschiedene solche Wurzeln gefunden, und somit geht folgender Satz hervor:

Ist die durch die Gleichung (23) ausgesprochene Bedingung erfüllt für jeden der in M'' enthaltenen verschiedenen Primfaktoren p, und bezeichnet μ die Anzahl dieser letzteren, so ist die Anzahl der Wurzeln der Congruenz (20) gleich 2^μ.

5. Nachdem in den vorigen beiden Nummern Bedingungen aufgestellt worden sind, welche zur eigentlichen Darstellbarkeit der Form φ durch die Form $f(x, x', x'')$ erforderlich sind, fragt es sich nun weiter, inwieweit diese Bedingungen hierzu auch genügen. Es werde also angenommen, die Form φ erfülle die letzteren, sie sei also primitiv, ihre Determinante sei $D = -\Omega M''$, wo M'' eine der Gleichung (14) genügende zu $2\Omega\Delta$ prime Zahl ist, und die Geschlechtscharaktere der Form φ entsprächen der Bedingungsgleichung (23). Aus dem letzteren Umstande folgt die Auflösbarkeit der Congruenz (20) d. h. das Vorhandensein ganzer Zahlen N, N' sowie M, M', N'', für welche die Gleichungen

$$(27) \qquad \Delta m = -N^2 + M'M'', \quad \Delta n'' = NN' - N''M'',$$
$$\Delta m' = -N'^2 + MM''$$

stattfinden, und aus diesen Gleichungen findet man mit Rücksicht auf die Gleichung

$$D = -\Omega M'' = n''^2 - mm'$$

einerseits

$$(28) \qquad MM'M'' + 2NN'N'' - MN^2 - M'N'^2 - M''N''^2 = \Omega\Delta^2$$

andererseits

$$\Delta(Mm + 2N''n'' + M'm') = \Omega\Delta^2 + M''(MM' - N''^2),$$

woraus ferner, da M'' prim gegen Δ vorausgesetzt ist,

$$(29) \qquad MM' - N''^2 = \Delta \cdot m'',$$

unter m'' eine ganze Zahl verstanden, hervorgeht. Setzt man nun

$$n'n'' - mn = \Omega N, \quad n''n - m'n' = \Omega N',$$

so folgen die Gleichungen

$$(30) \qquad M''n = -Nm' - N'n'', \quad M''n' = -Nn'' - N'm,$$

denen man, wenn man sie mit Δ multiplicirt und die Gleichungen (27) benutzt, folgende andere Form geben kann:

$$(31) \qquad \Delta n = N'N'' - NM, \quad \Delta n' = N''N - N'M'.$$

Hiernach sind n, n' rationale Zahlen, welche, auf die einfachste Benennung gebracht, zum Nenner wegen (30) nur einen Theiler von M'', wegen (31) nur einen Theiler von Δ haben können; da M'', Δ aber keinen gemeinsamen Theiler besitzen, so müssen n, n' ganze Zahlen sein. Endlich bemerke man, dass, weil jeder gemeinsame Theiler der fünf Zahlen M, M', N, N', N'' wegen (28) in $\Omega\Delta^2$ aufgehen muss, die sechs Zahlen M, M', M'', N, N', N'' keinen von 1 verschiedenen gemeinsamen Theiler haben können.

Aus alle diesem geht hervor, dass, wenn die primitive Form φ die gestellten Bedingungen erfüllt, es eine primitive Form

$$\mathfrak{F}_1 = \begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$$

mit der Determinante $\Omega\Delta^2$ giebt, deren Adjungirte nach den Gleichungen (27), (29) und (31) gleich

$$\begin{pmatrix} \Delta m, & \Delta m', & \Delta m'' \\ \Delta n, & \Delta n', & \Delta n'' \end{pmatrix}$$

ist und Δ zum grössten gemeinsamen Theiler aller Coefficienten hat, sodass die primitive Form

$$f_1 = \begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$$

umgekehrt $\Omega \cdot \mathfrak{F}_1$ zur Adjungirten und $\Omega^2\Delta$ zur Determinante hat; ihre Invarianten sind mithin jedenfalls $\pm\,\Omega$ und Δ. Um

sie genau zu bestimmen, bedenke man, dass nach der Voraussetzung im Falle $\Omega > 0$ d. h., wenn f eine bestimmte (positive) Form ist, auch φ eine positive Form, mithin $\Omega M''$ und m positiv sind; demnach ist auch f_1 (s. Capitel 1 nr. 2) eine bestimmte Form, ihre erste Invariante also positiv d. i. gleich $+\Omega$. Im Falle $\Omega < 0$ aber, d. h. wenn f eine unbestimmte Form ist, muss φ entweder negativ oder unbestimmt sein und folglich ist auch f_1 eine unbestimmte; dies leuchtet ein, wenn φ unbestimmt ist; ist aber φ negativ, so könnte die Form f_1, wenn sie eine bestimmte wäre, auch nur eine negative Form sein, was doch nicht möglich ist, da ihre Determinante positiv ist. Die erste Invariante von f_1 ist also wieder $+\Omega$. — So ist folgendes Resultat gewonnen:

Erfüllt eine binäre quadratische Form φ die zur eigentlichen Darstellbarkeit durch die Form $f(x, x', x'')$ der Ordnung (Ω, Δ) erforderlichen Bedingungen, so giebt es eine ternäre quadratische Form derselben Ordnung, welche φ als einen Bestandtheil enthält und in deren Reciproker der 3te, 4te und 5te Coefficient resp. gleich M'', N und N' sind, während N, N' irgend eine der Wurzeln der Congruenz (20) bedeuten.

6. Mit Hilfe dieses Ergebnisses können nunmehr die sämmtlichen eigentlichen Darstellungen einer gegebenen binären quadratischen Form φ durch eine gegebene ternäre Form, wenn es deren überhaupt giebt, ermittelt werden. Sei (Ω, Δ) die Ordnung der letztern Form und von der Form φ werde angenommen — weil sonst keine Darstellungen vorhanden sind — dass sie die zur Darstellbarkeit durch eine Form dieser Ordnung erforderlichen Bedingungen erfülle. Man denke sich die sämmtlichen ternären quadratischen Formen der Ordnung (Ω, Δ) in Classen äquivalenter Formen vertheilt und aus jeder dieser Classen eine einzelne Form als ihren Repräsentanten herausgegriffen; so erhält man ein System unter sich nicht äquivalenter Formen

$$f_1, f_2, f_3, \ldots, \tag{32}$$

welches das Formensystem der Ordnung (Ω, Δ) heisst. Aus nr. 3 vorigen Capitels folgt und wird sich auch später

zeigen (s. Abschnitt 3), dass die Anzahl der Formen, aus denen es besteht, eine endliche ist.

Nun ist nach der bezüglich φ gemachten Voraussetzung die Congruenz (20) erfüllbar und besitzt, wenn μ die Anzahl der verschiedenen Primfaktoren bezeichnet, aus denen M'' besteht, 2^μ verschiedene Wurzeln, als deren Repräsentanten die nachstehenden gewählt seien:

$$(N_1, N_1'),\quad (N_2, N_2'),\quad (N_3, N_3'), \ldots \tag{33}$$

Jedem derselben entsprechend giebt es nach voriger nr. je eine Form

$$f', f'', f''', \ldots \tag{34}$$

der Ordnung (Ω, Δ), welche φ als Bestandtheil enthält, und in deren Reciproker die 3ten, 4ten, 5ten Coefficienten resp.

$$M'',\ N_1,\ N_1';\ M'',\ N_2,\ N_2';\ \ldots$$

sind. Jede dieser Formen, z. B. $f^{(i)}$, ist mit einer einzigen Form des Systems (32) äquivalent. Ist etwa f_1 diese äquivalente Form, so wird jede ganzzahlige Transformation

$$\left\{\begin{aligned} x &= \alpha_0{}^0 y + \alpha_0{}' y' + \alpha_0{}'' y'' \\ x' &= \alpha_1{}^0 y + \alpha_1{}' y' + \alpha_1{}'' y'' \\ x'' &= \alpha_2{}^0 y + \alpha_2{}' y' + \alpha_2{}'' y'', \end{aligned}\right. \tag{35}$$

welche f_1 in $f^{(i)}$ verwandelt, eine eigentliche Darstellung von φ durch f_1 liefern vermittelst der Formeln

$$\left\{\begin{aligned} x &= \alpha_0{}^0 y + \alpha_0{}' y' \\ x' &= \alpha_1{}^0 y + \alpha_1{}' y' \\ x'' &= \alpha_2{}^0 y + \alpha_2{}' y', \end{aligned}\right. \tag{36}$$

und diese Darstellung gehört zur Wurzel (N_i, N_i'), da die zu f_1 Reciproke $\mathfrak{F}_1$ alsdann durch die Substitution

$$\begin{aligned} x &= \mathsf{A}_0{}^0 y + \mathsf{A}_0{}' y' + \mathsf{A}_0{}'' y'' \\ x' &= \mathsf{A}_1{}^0 y + \mathsf{A}_1{}' y' + \mathsf{A}_1{}'' y'' \\ x'' &= \mathsf{A}_2{}^0 y + \mathsf{A}_2{}' y' + \mathsf{A}_2{}'' y'' \end{aligned}$$

in die Reciproke von $f^{(i)}$ übergeht, also die Gleichungen stattfinden:

$$\begin{aligned} N_i &= \mathsf{A}_0{}' \mathfrak{F}_1{}^0(\mathsf{A}'') + \mathsf{A}_1{}' \mathfrak{F}_1{}^1(\mathsf{A}'') + \mathsf{A}_2{}' \mathfrak{F}_1{}^2(\mathsf{A}'') \\ N_i' &= \mathsf{A}_0{}^0 \mathfrak{F}_1{}^0(\mathsf{A}'') + \mathsf{A}_1{}^0 \mathfrak{F}_1{}^1(\mathsf{A}'') + \mathsf{A}_2{}^0 \mathfrak{F}_1{}^2(\mathsf{A}''). \end{aligned}$$

Auf solche Weise muss aber auch jede eigentliche, zur Wurzel (N_i, N_i') gehörige Darstellung von φ durch eine der Formen (32) erhalten werden. Denn diejenige dieser Formen, durch welche solche Darstellung erfolgt, ist nach nr. 3 einer Form äquivalent, welche φ zum Bestandtheile hat, und in deren Reciproken der 3te, 4te, 5te Coefficient resp. M'', N_i, N_i' sind; die übrigen Coefficienten der Form und ihrer Reciproken aber ergeben sich dann mittels der Gleichungen

$$\Delta m = M_i' M'' - N_i^2, \quad \Delta n'' = N_i N_i' - N_i'' M''$$

$$\Delta m' = M_i M'' - N_i'^2,$$

dann

$$\Delta m_i'' = - N_i''^2 + M_i M_i'$$

und endlich

$$\Delta n_i = N_i' N_i'' - N_i M_i, \quad \Delta n_i' = N_i'' N_i - N_i' M_i',$$

deren Vergleichung mit den Formeln (27), (29), (31) die gedachte Form als identisch mit $f^{(i)}$ erweist. Somit ist diejenige der Formen (32), durch welche die zur Wurzel (N_i, N_i') gehörige Darstellung von φ erfolgt, die Form f_1. Heisst nun (36) diese Darstellung, so geht f_1 in $f^{(i)}$ durch eine Substitution (35) über und die Darstellung muss folglich unter den vorher angegebenen befindlich sein.

Führt man diese Betrachtung für jede derjenigen Formen (34) durch, welche mit ein- und derselben Form des Systems (32), z. B. f_1, äquivalent sind, so erhält man die sämmtlichen eigentlichen Darstellungen, deren die Form φ durch diese Form f_1 fähig ist. Da man aber bei Aufstellung des Systems (32) jede beliebig gegebene Form f der Ordnung (Ω, Δ) als Repräsentanten ihrer Classe einführen kann, so lassen sich auf die angegebene Weise die sämmtlichen eigentlichen Darstellungen der binären Form φ durch eine *gegebene* ternäre *Form* f überhaupt ermitteln.

Hier soll hinzugefügt werden, dass alle so erhaltenen Darstellungen der Form φ auch von einander verschieden sind. Sonst müsste nämlich eine der Formen (34), etwa f', aus der gedachten Form f durch eine Substitution

$$\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix},$$

und eine der Formen (34), welche auch mit f' identisch sein kann — sie werde f'' genannt — aus f durch eine Substitution

$$\begin{pmatrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{pmatrix}$$

hervorgehen, welche dieselbe erste und zweite, aber eine verschiedene dritte Vertikalreihe hat. Da nun, wenn zur Abkürzung

$$\alpha'\beta'' - \alpha''\beta' = \mathsf{A}, \quad \alpha''\beta - \alpha\beta'' = \mathsf{A}', \quad \alpha\beta' - \alpha'\beta = \mathsf{A}''$$

gesetzt wird,

$$\mathsf{A}\gamma + \mathsf{A}'\gamma' + \mathsf{A}''\gamma'' = 1, \quad \mathsf{A}\delta + \mathsf{A}'\delta' + \mathsf{A}''\delta'' = 1$$

ist, so müssen, unter h, h', h'' Unbestimmte verstanden, Gleichungen bestehen von der Form

$$\delta = \gamma + h'\mathsf{A}'' - h''\mathsf{A}', \; \delta' = \gamma' + h''\mathsf{A} - h\mathsf{A}'', \; \delta'' = \gamma'' + h\mathsf{A}' - h'\mathsf{A}.$$

Setzt man ferner

$$\mathfrak{A} = h\alpha + h'\alpha' + h''\alpha'', \quad \mathfrak{B} = h\beta + h'\beta' + h''\beta'',$$

so findet sich ohne Schwierigkeit, dass f'' in f durch die Substitution

$$\begin{pmatrix} \beta'\gamma'' - \beta''\gamma' - \mathfrak{B}\mathsf{A}, & \beta''\gamma - \beta\gamma'' - \mathfrak{B}\mathsf{A}', & \beta\gamma' - \beta'\gamma - \mathfrak{B}\mathsf{A}'' \\ \gamma'\alpha'' - \gamma''\alpha' + \mathfrak{A}\mathsf{A}, & \gamma''\alpha - \gamma\alpha'' + \mathfrak{A}\mathsf{A}', & \gamma\alpha' - \gamma'\alpha + \mathfrak{A}\mathsf{A}'' \\ \mathsf{A}, & \mathsf{A}', & \mathsf{A}'' \end{pmatrix}$$

und folglich f'' in f' durch die folgende:

$$\begin{pmatrix} 1, & 0, & -\mathfrak{B} \\ 0, & 1, & \mathfrak{A} \\ 0, & 0, & 1 \end{pmatrix}$$

übergehen würde. Demnach ginge die Reciproke von f' durch die transponirte Substitution

$$\begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ -\mathfrak{B}, & \mathfrak{A}, & 1 \end{pmatrix}$$

in die Reciproke von f'' über, deren 4ter und 5ter Coefficient deshalb, wie sogleich zu übersehen, mit den entsprechenden der ersteren Reciproke (mod. M'') congruent sein würde. Dies widerspräche der Herleitung der Formen (34), es sei denn, dass f'' identisch mit f', eine Voraussetzung, welche erfordern würde, dass

$$\mathfrak{A} = h\alpha + h'\alpha' + h''\alpha'' = 0, \quad \mathfrak{B} = h\beta + h'\beta' + h''\beta'' = 0$$

ist, woraus dann

$$\begin{array}{lll} h'\mathsf{A}'' - h''\mathsf{A}' = 0 & \text{also} & \delta = \gamma \\ h''\mathsf{A} - h\mathsf{A}'' = 0 & \quad " & \delta' = \gamma' \\ h\mathsf{A}' - h'\mathsf{A} = 0 & \quad " & \delta'' = \gamma'' \end{array}$$

folgen würde, gegen die Voraussetzung.

Führt man dagegen die angestellte Betrachtung für jede der Formen (34) insgesammt durch, so findet man die sämmtlichen eigentlichen Darstellungen, deren φ durch das ganze Formen*system* der Ordnung (Ω, Δ) fähig ist.

Durch diese Erörterungen ist aber schliesslich die Aufgabe, alle solche Darstellungen einer binären quadratischen Form und nach nr. 2 also auch die Aufgabe, alle Darstellungen einer Zahl durch eine ternäre quadratische Form zu finden, auf die beiden andern Aufgaben zurückgeführt:

erstens: über die Aequivalenz oder Nichtäquivalenz zweier Formen derselben Ordnung zu entscheiden und

zweitens: im Falle der Aequivalenz sämmtliche ganzzahligen Transformationen der einen in die andere anzugeben.

Die erstere dieser Aufgaben wird im dritten Abschnitte mittels der sogenannten reducirten Formen gelöst werden. Da nun durch Feststellung der Aequivalenz stets eine Transformation der einen Form in die andere gefunden wird und ferner (s. nr. 5 des ersten Capitels) aus einer solchen sämmtliche sich ergeben, sobald man sämmtliche ganzzahlige Transformationen einer von ihnen in sich selbst kennt, so wird man an Stelle der zweiten Aufgabe diese andere setzen dürfen:

Alle ganzzahligen Transformationen einer gegebenen ternären quadratischen Form in sich selbst zu ermitteln.

Was bezüglich dieser Aufgabe bisher geleistet worden ist, soll im nächsten Capitel dargestellt werden.

Viertes Capitel.

Die ganzzahligen Transformationen einer ternären quadratischen Form in sich selbst.

1. Im ersten Capitel sind die Formeln hergeleitet, welche die sämmtlichen Transformationen einer gegebenen ternären quadratischen Form in sich selbst darstellen. Die Aufgabe wird nun sein, festzustellen, in welcher Weise die in jenen Formeln auftretenden Unbestimmten p, q, q', q'' zu beschränken sind, damit die Transformation ganzzahlig wird.

Man ersieht zuvörderst aus den Gleichungen (59) und (61) daselbst, dass die mit t, u, u', u'' bezeichneten Grössen alsdann nothwendig rational sein müssen, und folglich muss man gemäss den dortigen Gleichungen (65) die Grössen p, q, q', q'' von folgender Gestalt voraussetzen:

$$p = \frac{\pi}{\lambda}\sqrt{\nu}, \quad q = \frac{\varkappa}{\lambda}\sqrt{\nu}, \quad q' = \frac{\varkappa'}{\lambda}\sqrt{\nu}, \quad q'' = \frac{\varkappa''}{\lambda}\sqrt{\nu},$$

in welcher $\lambda, \nu, \pi, \varkappa, \varkappa', \varkappa''$ ganze Zahlen bedeuten. Da nun p, q, q', q'' durch die Gleichung

$$p^2 + F(q, q', q'') = 1$$

mit einander verbunden sind, die linken Seiten der dortigen Gleichungen (70) demnach auch mit $p^2 + F(q, q', q'')$ multiplicirt gedacht und statt $2p^2 - 1$ auch $p^2 - F(q, q', q'')$ gesetzt werden darf, so hebt sich die Irrationalität und der Generalnenner rechts und links heraus und man darf sagen: Die Grössen p, q, q', q'' dürfen in den Formeln (70) als ganzzahlig gedacht werden, wenn man links mit

$$P = p^2 + F(q, q', q'') \tag{1}$$

multiplicirt; zur Aufstellung der ganzzahligen Transformationen aber wird es darauf ankommen, welche Werthe diese Zahl P erhalten darf, wenn die neun Coefficienten in den folgenden Gleichungen:

$$(2)\quad \begin{cases} \qquad (p^2 + F(q,q',q''))\cdot x \\ = (p^2 - F(q,q',q'') + 2pq'b' - 2pq''b'' + 2qF^0(q))\cdot y \\ + (2pq'b - 2pq''a' + 2q'F^0(q))\cdot y' \\ + (2pq'a'' - 2pq''b + 2q''F^0(q))\cdot y'' \\ \qquad (p^2 + F(q,q',q''))\cdot x' \\ = (2pq''a - 2pqb' + 2qF^1(q))\cdot y \\ + (p^2 - F(q,q',q'') + 2pq''b'' - 2pqb + 2q'F^1(q))\cdot y' \\ + (2pq''b' - 2pqa'' + 2q''F^1(q))\cdot y'' \\ \qquad (p^2 + F(q,q',q''))\cdot x'' \\ = (2pqb'' - 2pq'a + 2qF^2(q))\cdot y \\ + (2pqa' - 2pq'b'' + 2q'F^2(q))\cdot y' \\ + (p^2 - F(q,q',q'') + 2pqb - 2pq'b' + 2q''F^2(q))\cdot y'' \end{cases}$$

nach Division mit P ganzzahlig werden sollen. Wegen der Homogeneïtät dieser Formeln leuchtet ein, dass man p, q, q', q'' ohne gemeinsamen Theiler voraussetzen darf. Bezeichnet man dann die neun Coefficienten in den vorigen Gleichungen der Reihe nach kurz durch (1), (2), ... (9), so finden sich unmittelbar, wenn für den Augenblick unter D wieder die Determinante der ternären quadratischen Form verstanden wird, die Beziehungen:

$$\begin{aligned} (1) + (5) + (9) &= 4p^2 - P \\ a\cdot(1) + b''\cdot(4) + b'\cdot(7) &= a(p^2 - F) + 2Dq^2 \\ b''\cdot(2) + a'\cdot(5) + b\cdot(8) &= a'(p^2 - F) + 2Dq'^2 \\ b'\cdot(3) + b\cdot(6) + a''\cdot(9) &= a''(p^2 - F) + 2Dq''^2, \end{aligned}$$

aus welchen sich folgende Congruenzen

$$(3)\quad \left\{\begin{matrix} 4p^2 \equiv 0, & 2ap^2 + 2Dq^2 \equiv 0, \\ 2a'p^2 + 2Dq'^2 \equiv 0, & 2a''p^2 + 2Dq''^2 \equiv 0 \end{matrix}\right\} (\text{mod. } P)$$

als nothwendige Bedingungen für ganzzahlige Transformationen ergeben. Man schliesst daraus vor Allem, dass $4Dp^2$, $4Dq^2$,

$4Dq'^2$, $4Dq''^2$ durch P theilbar sein müssen, und da p, q, q', q'' keinen gemeinsamen Theiler haben, muss P ein Theiler von $4D$ sein.

2. Dies Resultat ergab sich, ohne dass irgend welche besondere Voraussetzungen einzuführen waren. Man bemerke jetzt aber, dass es gar nicht erforderlich ist, unsere Aufgabe in allgemeinster Weise zu lösen. Sind nämlich f und f_1 zwei äquivalente Formen, so folgt aus dem allgemeinen in nr. 5 des ersten Capitels gegebenen Satze, dass man sämmtliche ganzzahlige Transformationen von f_1 in sich selbst erhält, wenn man eine ganzzahlige Transformation von f_1 in f mit allen ganzzahligen Transformationen von f in sich selbst, und die so entstehenden Transformationen mit einer ganzzahligen Transformation von f in f_1 zusammensetzt. Sieht man also die Aufgabe, über die Aequivalenz zweier Formen zu entscheiden, durch deren Lösung zugleich eine Transformation von f in f_1 und umgekehrt erhalten wird, als gelöst an, so bedarf es nur noch der Ermittelung aller ganzzahligen Transformationen von f in sich selbst, und somit kann man sich die Aufgabe zu erleichtern suchen, indem man in der Classe von f_1 eine besonders geeignete Form f aufsucht. Diese Bemerkung wollen wir uns zu Nutze machen, indem wir — uns wieder auf eigentlich-primitive Formen beschränkend — dem in nr. 7 des zweiten Capitels gegebenen Satze von Smith gemäss die Form f so voraussetzen, dass sie den Congruenzen

$$\left.\begin{cases} f \equiv \alpha x^2 + \alpha'\Omega x'^2 + \alpha''\Omega\Delta x''^2 \\ 1 \equiv \alpha\alpha'\alpha'' \end{cases}\right\} \pmod{4\Omega\Delta}, \tag{4}$$

während

$$\alpha\Delta \equiv 1 \pmod{4}$$

gedacht wird, genügt; daraus folgt dann, dass die Coefficienten b, b', b'' der Form

$$f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

gerade, dagegen a, a', a'' ungerade, also auch B, B', B'' gerade, A, A', A'' ungerade sind, während wegen der aus (4) folgenden Congruenzen

$$A \equiv \alpha'\alpha''\Delta,\ A' \equiv \alpha\alpha''\Omega\Delta,\ A'' \equiv \alpha\alpha'\Omega \pmod 4$$

(5) $$AA'A'' \equiv 1 \pmod 4$$

gefunden wird.

Ferner aber wollen wir nur den Fall hier durchführen, in welchem die Determinante der Form keine quadratischen Theiler hat, mithin gleich Δ ist.

Unter diesen Umständen muss P von der Form $2^\lambda \Delta_0$ sein, wo Δ_0 ein Theiler von Δ und λ eine der Zahlen 0, 1 oder 2 ist, und die Gleichung, der p, q, q', q'' genügen müssen, wird sich folgendermassen schreiben lassen:

(6) $$p^2 + F(q, q', q'') = 2^\lambda \Delta_0;$$

die erste der Congruenzen (3) aber erfordert noch, dass p^2, und da Δ_0 aus lauter verschiedenen Primfaktoren besteht, auch p selbst durch Δ_0 theilbar sei. Ist $\lambda = 2$, so ergiebt sich aus den übrigen jener Congruenzen, dass p, q, q', q'' ungerade Zahlen sein müssen.

Diese nothwendigen Bedingungen ganzzahliger Transformationen sind aber zugleich auch hinreichend. In der That, sind für irgend ein System der Werthe λ, Δ_0, wie sie definirt worden, p, q, q', q'' eine Lösung der Gleichung (6), bei welcher p theilbar ist durch Δ_0, so folgt zunächst auch

$$F(q, q', q'') \equiv 0 \pmod{\Delta_0}$$

und hieraus mittels der zweiten Grundformel:

$$\begin{aligned} & F(x, x', x'') \cdot F(q, q', q'') \\ = & (xF^0(q) + x'F^1(q) + x''F^2(q))^2 \\ & + \Delta \cdot f(x'q'' - x''q', x''q - xq'', xq' - x'q) \end{aligned}$$

für alle ganzzahligen x, x', x'' die Congruenz

$$xF^0(q) + x'F^1(q) + x''F^2(q) \equiv 0 \pmod{\Delta_0}$$

mithin insbesondere

(7) $$F^0(q) \equiv 0,\quad F^1(q) \equiv 0,\quad F^2(q) \equiv 0 \pmod{\Delta_0}.$$

Hiernach werden die sämmtlichen Coefficienten der Transformation (2) durch Δ_0 theilbar sein. Ist nun ferner zunächst $\lambda = 0$ oder 1, so sind sie, da

$$p^2 - F(q, q', q'') = 2p^2 - P$$

gesetzt werden darf, auch sämmtlich theilbar durch 2^λ. Ist

aber $\lambda = 2$, so sind, wenn p, q, q', q'' eine Auflösung der Gleichung (6) in ungeraden Zahlen bedeuten, nicht nur die in b, b', b'' multiplicirten Theile der Coefficienten durch $2^\lambda = 4$ theilbar, sondern auch ihre übrigen Bestandtheile, welche sich, da

$$(8) \qquad \begin{cases} F^0(q) = Aq + B''q' + B'q'' \\ F^1(q) = B''q + A'q' + Bq'' \\ F^2(q) = B'q + Bq' + A''q'' \end{cases}$$

ungerade sind, als doppelte Summe zweier ungeraden Zahlen darstellen. Also sind jederzeit unter den für p, q, q', q'' gemachten Voraussetzungen sämmtliche Coefficienten der Transformation (2) durch P theilbar, diese Transformation mithin eine ganzzahlige.

Man bemerke hier noch, dass für $\lambda = 2$ und ungerade p, q, q', q'' aus der Gleichung (6) die Congruenz

$$A + A' + A'' + 2(B + B' + B'') \equiv 3 \pmod{8}$$

hervorgeht, der man mit Rücksicht auf die Voraussetzungen über die Form f leicht die andere Form

$$a'a'' + a''a + aa' \equiv 3 \pmod{8}$$

geben kann. Nun ist nach diesen Voraussetzungen

$$AA'A'' \equiv 1 \pmod{4}$$

also entweder jede der Zahlen A, A', A'' congruent 1, oder eine von ihnen, etwa A, congruent 1, die beiden andern congruent 3 (mod. 4). Im letzteren Falle aber würden

$$a' = 4\mathfrak{a}' \pm 1, \quad a'' = 4\mathfrak{a}'' \pm 1, \quad a = 4\mathfrak{a} \mp 1$$

und demnach

$$a'a'' + a''a + aa' \equiv -1 \pmod{8}$$

sein. Da dies der zuerst erhaltenen Congruenz widerspricht, so ersieht man, dass die Gleichung (6) für $\lambda = 2$ nur in Betracht kommt, so oft A, A', A'' sämmtlich congruent 1 sind (mod. 4).

3. Die soeben erhaltenen Ergebnisse gelten sowohl für bestimmte als für unbestimmte ternäre Formen. Doch unterscheiden sich diese beiden Arten von Formen nun wesentlich durch den Umstand, dass die ersteren nur eine endliche, die letzteren dagegen eine unendliche

Menge von Transformationen in sich selbst besitzen. Wenn wir nämlich zuvörderst f also auch F als eine bestimmte (positive) Form voraussetzen, so hat in der That jede der Gleichungen (6), deren es ebenso wie der zulässigen Werthsysteme λ, Δ_0 nur eine endliche Menge giebt, auch nur eine endliche Anzahl ganzzahliger Auflösungen. Denn für jede solche Gleichung bleibt die positive Zahl $F(q, q', q'')$ also auch, wenn

$$Aq + B''q' + B'q'' = \mathfrak{q}, \quad a''q' - bq'' = \mathfrak{q}', \quad q'' = \mathfrak{q}''$$

gesetzt wird, der Ausdruck

$$a''A \cdot F(q, q', q'') = a''\mathfrak{q}^2 + \Delta\mathfrak{q}'^2 + \Delta A \cdot \mathfrak{q}''^2$$

unter einer endlichen Grenze und folglich sind für die ganzen Zahlen $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}''$ sowie für die ihnen etwa entsprechenden ganzen Zahlen q, q', q'' nur eine endliche Menge von Werthen zulässig. Ist dagegen f und folglich auch F eine unbestimmte Form und

$$F(\gamma, \gamma', \gamma'') = -M$$

irgend eine negative durch F darstellbare ganze Zahl, so erhält für jede solche ganze Zahl die Gleichung

$$p^2 + F(q, q', q'') = 1$$

unendlich viel ganzzahlige Auflösungen

$$p = t, \quad q = \gamma u, \quad q' = \gamma' u, \quad q'' = \gamma'' u,$$

indem man t, u der Gleichung

$$t^2 - M \cdot u^2 = 1$$

gemäss wählt, und liefert schon allein für diesen einen Werth von F unendlich viel Transformationen von f in sich selbst.

Später (s. zweiten Abschnitt, Cap. 10) wird gezeigt werden, dass z. B. für die positive Form

$$f(x, x', x'') = x^2 + x'^2 + x''^2 \tag{9}$$

die Anzahl aller Transformationen in sich selbst gleich 24 ist, und werden diese Transformationen selbst bestimmt werden. Es ist nicht ohne Interesse, zu sehen, wie dieselben aus der allgemeinen hier dargestellten Theorie zu gewinnen sind. Man beachte dabei, dass p, wenn von Null verschieden, positiv zu nehmen, und dass, wenn $p = 0$, von den zwei Systemen

$$q, q', q'' \quad \text{und} \quad -q, -q', -q''$$

nur das erstere beizubehalten ist. Der Form (9) entspricht $\Delta = 1$ und als Adjungirte die Form

$$F(x, x', x'') = x^2 + x'^2 + x''^2,$$

man hat folglich $A \equiv A' \equiv A'' \equiv 1 \pmod{4}$ und die Gleichung (6) steht an Stelle der folgenden drei:

1) $$p^2 + q^2 + q'^2 + q''^2 = 1$$

mit den vier Lösungen

$$\begin{array}{cccc} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1; \end{array}$$

2) $$p^2 + q^2 + q'^2 + q''^2 = 2$$

mit den sechs Lösungen

$$\begin{array}{cccc} 1, & \pm 1, & 0, & 0 \\ 1, & 0, & \pm 1, & 0 \\ 1, & 0, & 0, & \pm 1 \end{array}$$

mit positivem p, und den sechs Lösungen

$$\begin{array}{cccc} 0, & \pm 1, & 1, & 0 \\ 0, & 0, & \pm 1, & 1 \\ 0, & 1, & 0, & \pm 1 \end{array}$$

mit verschwindendem p;

3) $$p^2 + q^2 + q'^2 + q''^2 = 4$$

mit den acht Lösungen in ungeraden ganzen Zahlen

$$1, \quad \pm 1, \quad \pm 1, \quad \pm 1,$$

denen ebensoviel verschiedene Transformationen entsprechen. Die Form (9) hat demnach in der That 24 Transformationen in sich selbst.

4. Wesentlich grössere Bedeutung, als für die bestimmten, hat die Theorie der Gleichung (6) für die unbestimmten ternären Formen. Hier gilt zunächst folgende Regel, um für ein bestimmtes Werthsystem λ, Δ_0 aus *einer* Auflösung der Gleichung

(6) $$p^2 + F(q, q', q'') = 2^\lambda \Delta_0,$$

bei welcher $p \equiv 0 \pmod{\Delta_0}$ und p, q, q', q'', so oft $\lambda = 2$ ist, ungerade Zahlen sind, *sämmtliche* Auflösungen dieser Gleichung von derselben Beschaffenheit zu finden:

Man bilde nach der in nr. 3 des ersten Capitels gegebenen Regel das Produkt

(10) $$(t^2 + F(u, u', u'')) \cdot (p^2 + F(q, q', q'')) = p_1^2 + F(q_1, q_1', q_1''),$$

indem man für t, u, u', u'' sämmtliche ganzzahlige Lösungen der Gleichung

(11) $$t^2 + F(u, u', u'') = 1,$$

sowie, falls $\lambda = 1$ oder 2 ist, auch sämmtliche ganzzahlige Lösungen der Gleichung

(11a) $$t^2 + F(u, u', u'') = 4$$

in ungeraden Zahlen einsetzt, werfe diejenigen so entstehenden Systeme p_1, q_1, q_1', q_1'' fort, welche durch 4 theilbar sind, und nehme von denjenigen der übrigen, die durch 2 theilbar sind, die Hälfte, so sind die so erhaltenen nicht durch 2 theilbaren Systeme p_1, q_1, q_1', q_1'' sowie die halben anderen:

$$\frac{p_1}{2}, \frac{q_1}{2}, \frac{q_1'}{2}, \frac{q_1''}{2}$$

sämmtliche gesuchte Lösungen der Gleichung (6).

Um dies zu beweisen, bemerke man erstens, dass die angeführte Regel für p_1, q_1, q_1', q_1'' folgende Werthe ergiebt:

(12) $$\begin{cases} p_1 = tp - u \cdot F^0(q) - u' \cdot F^1(q) - u'' \cdot F^2(q) \\ q_1 = tq + pu + f^0(u'q'' - u''q') \\ q_1' = tq' + pu' + f^1(u'q'' - u''q') \\ q_1'' = tq'' + pu'' + f^2(u'q'' - u''q'). \end{cases}$$

Die erste dieser Formeln zeigt im Hinblick auf die Congruenzen (7), dass p_1, gleichviel ob t, u, u', u'' eine Lösung von (11) oder von (11a) darstellen, durch Δ_0 theilbar ist. Wenn also t, u, u', u'' eine Lösung der ersteren dieser Gleichungen, so bilden p_1, q_1, q_1', q_1'' wegen (10) jedenfalls eine

Lösung der Gleichung (6) und zwar, falls $\lambda = 2$ ist, eine Lösung in ungeraden Zahlen; denn in diesem Falle sind p, q, q', q'' ungerade und aus den letzten Formeln ergiebt sich unter den von uns gemachten Voraussetzungen jede der Zahlen p_1, q_1, q_1', q_1'' congruent

$$t + u + u' + u'' \pmod{2},$$

während wegen (11)

$$t^2 + u^2 + u'^2 + u''^2$$

und folglich auch

$$t + u + u' + u'' \equiv 1 \pmod{2}$$

gefunden wird. — Ist dagegen t, u, u', u'' eine ungerade Auflösung der Gleichungen (11a), so folgt zunächst

$$(13) \qquad p_1^2 + F(q_1, q_1', q_1'') = 4 \cdot 2^\lambda \Delta_0,$$

aber die Gleichungen (12) liefern die Congruenzen

$$p_1 \equiv q_1 \equiv q_1' \equiv q_1'' \equiv p + q + q' + q'' \pmod{2},$$

während für $\lambda = 1$ oder 2 aus (6) $p^2 + q^2 + q'^2 + q''^2$ also auch

$$p + q + q' + q'' \equiv 0 \pmod{2}$$

hervorgeht; somit sind p_1, q_1, q_1', q_1'' gerade Zahlen und

$$\frac{p_1}{2}, \frac{q_1}{2}, \frac{q_1'}{2}, \frac{q_1''}{2}$$

bilden jedenfalls eine ganzzahlige Auflösung der Gleichung (6). Indessen ereignet sich, wenn $\lambda = 2$ ist, der Fall, dass diese Auflösung eine solche in geraden Zahlen wird. In der That folgt, da in diesem Falle $A \equiv A' \equiv A'' \equiv 1 \pmod{4}$ ist und p_1, q_1, q_1', q_1'' gerade sind, aus der Gleichung (13) die Congruenz

$$p_1^2 + q_1^2 + q_1'^2 + q_1''^2 \equiv 0 \pmod{16},$$

welche lehrt, dass entweder p_1, q_1, q_1', q_1'' sämmtlich von der Form $4n + 2$ oder sämmtlich von der Form $4n$ sein müssen. Bildet man andererseits den Werth von p_1 nicht nur für die Lösung t, u, u', u'', sondern auch für die Lösung

$$t, \; -u, \; -u', \; -u'',$$

so unterscheiden sich beide Werthe von p_1 nach der ersten der Formeln (12) um

$$2(uF^0(q) + u'F^1(q) + u''F^2(q)),$$

d. i. (mod. 4) um

$$2(uq + u'q' + u''q'') \equiv 2;$$

ist also einer jener Werthe von p_1 congruent 2, so ist der andere congruent 0 (mod. 4) und die zu ihm gehörigen Zahlen $\frac{p_1}{2}, \frac{q_1}{2}, \frac{q_1'}{2}, \frac{q_1''}{2}$ gerade. Werden aber solche Systeme p_1, q_1, q_1', q_1'' weggeworfen, so bilden für $\lambda = 2$ die übrigen Systeme $\frac{p_1}{2}, \frac{q_1}{2}, \frac{q_1'}{2}, \frac{q_1''}{2}$ eine Auflösung der Gleichung (6) in ungeraden Zahlen.

Aus diesen Betrachtungen ist zuerst zu erschliessen, dass die nach der ausgesprochenen Regel gefundenen Systeme

$$p_1, q_1, q_1', q_1'' \quad \text{resp.} \quad \frac{p_1}{2}, \frac{q_1}{2}, \frac{q_1'}{2}, \frac{q_1''}{2}$$

sämmtlich Lösungen der Gleichung (6) von der verlangten Beschaffenheit *sind.*

Zweitens kann man aus je zweien der bezeichneten Auflösungen p, q, q', q'' und r, s, s', s'' der Gleichung (6) auf folgende Weise je nach den verschiedenen Fällen, welche λ darbieten kann, eine Auflösung der Gleichung (11) resp. eine ungerade Auflösung der Gleichung (11a) herleiten. Man bezeichne mit S diejenige Transformation der Form f in sich selbst, welche aus den Elementen $p, -q, -q', -q''$, mit S_1 diejenige, welche aus den Elementen r, s, s', s'' gebildet ist. Setzt man dann

$$(14) \quad \begin{cases} R = pr + sF^0(q) + s'F^1(q) + s''F^2(q) = d \cdot t \\ Q = ps - rq + f^0(q's'' - q''s') = d \cdot u \\ Q' = ps' - rq' + f^1(q's'' - q''s') = d \cdot u' \\ Q'' = ps'' - rq'' + f^2(q's'' - q''s') = d \cdot u'', \end{cases}$$

wo d den grössten gemeinsamen Theiler von R, Q, Q', Q'' bezeichnet, sodass t, u, u', u'' vier ganze Zahlen ohne gemeinsamen Theiler bedeuten, so ist, wie nach der Regel in nr. 3 des ersten Capitels sogleich einleuchtet,

$$R^2 + F(Q, Q', Q'')$$
$$= (r^2 + F(s, s', s'')) \cdot (p^2 + F(-q, -q', -q''))$$

d. i.

$$(15) \qquad t^2 + F(u, u', u'') = \frac{2^{2\lambda} \cdot \Delta_0^2}{d^2},$$

und die Zahlen t, u, u', u'' sind nach Ende des ersten Capitels die Elemente derjenigen Transformation der Form f in sich selbst, welche aus der Zusammensetzung der Transformation S_1 und S resultirt. Demnach muss

$$\frac{2^{2\lambda} \Delta_0^2}{d^2} = 2^{\lambda_1} \cdot \Delta_1$$

sein, wo Δ_1 ein Theiler von Δ und λ_1 eine der Zahlen 0, 1 oder 2 ist, und falls $\lambda_1 = 2$ ist, müssen t, u, u', u'' ungerade Zahlen sein. Da nun Δ ungerade und ohne quadratische Theiler vorausgesetzt ist, ergiebt sich hieraus vor allem

$$\Delta_1 = 1.$$

Ist ferner $\lambda = 0$, so muss auch $\lambda_1 = 0$ sein, man erhält $\frac{2^\lambda \Delta_0}{d} = \pm 1$ und die Gleichung (15) nimmt die Gestalt an:

$$t^2 + F(u, u', u'') = 1.$$

Ist zweitens $\lambda = 1$ oder 2, so kann nur entweder $\lambda_1 = 0$, also $\frac{2^\lambda \Delta_0}{d} = \pm 1$ sein, und t, u, u', u'' befriedigen wieder die vorstehende Gleichung, oder es ist $\lambda_1 = 2$ also $\frac{2^\lambda \Delta_0}{d} = \pm 2$ und t, u, u', u'' sind eine ungerade Auflösung der Gleichung

$$t^2 + F(u, u', u'') = 4.$$

Vermittelst dieser so gefundenen Auflösung t, u, u', u'' der jedesmal bezeichneten Gleichung lassen sich nun durch eine einfache Rechnung aus den Formeln (14) die Zahlen r, s, s', s'' folgendermassen ausdrücken:

$$\begin{aligned}
\frac{2^\lambda \Delta_0}{d} \cdot r &= tp - uF^0(q) - u'F^1(q) - u''F^2(q) \\
\frac{2^\lambda \Delta_0}{d} \cdot s &= tq + pu - f^0(q'u'' - q''u') \\
\frac{2^\lambda \Delta_0}{d} \cdot s' &= tq' + pu' - f^1(q'u'' - q''u') \\
\frac{2^\lambda \Delta_0}{d} \cdot s'' &= tq'' + pu'' - f^2(q'u'' - q''u');
\end{aligned}$$

wenn man also, je nachdem $\frac{2^\lambda \Delta_0}{d} = \pm 1$ oder ± 2 ist

oder

$$r = \pm p_1, \quad s = \pm q_1, \quad s' = \pm q_1', \quad s'' = \pm q_1''$$

$$r = \pm \frac{p_1}{2}, \quad s = \pm \frac{q_1}{2}, \quad s' = \pm \frac{q_1'}{2}, \quad s'' = \pm \frac{q_1''}{2}$$

setzt, so zeigen die letzterhaltenen Formeln, dass die Zahlen p_1, q_1, q_1', q_1'' aus p, q, q', q'' und t, u, u', u'' durch die Entwickelung des Produkts (10) nach der früher gegebenen Regel entstehen, und man sieht somit zweitens, dass *jede* der verlangten Lösungen r, s, s', s'' der Gleichung (6) nach der oben gegebenen Regel gefunden wird.

Demnach ist diese Regel in ihrem ganzen Umfange begründet.

5. Die Gleichung (6) vertritt die Stelle von so viel verschiedenen Gleichungen, als es Combinationen der Werthe für λ und Δ_0 giebt; da bei unbestimmten Formen Δ_0 jeden positiven wie negativen Theiler von Δ bezeichnet, beträgt diese Anzahl von Combinationen oder Gleichungen, wenn $T(\Delta)$ die Anzahl der positiven Theiler von Δ bedeutet,

$$4 \cdot T(\Delta) \quad \text{oder} \quad 6 \cdot T(\Delta),$$

je nachdem von den drei Coefficienten A, A', A'' nur einer oder alle drei von der Form $4n + 1$ sind. Ob alle diese Gleichungen wirklich in der angegebenen Weise lösbar sind, kann hier noch nicht erörtert, wird aber später in bejahendem Sinne beantwortet werden. Und somit lässt sich aus der in voriger nr. angestellten Betrachtung folgender Schluss ziehen:

Bezeichnet man mit $S_0, S_1, S_2, \ldots$ die stets in endlicher Anzahl vorhandenen singulären Transformationen, welche aus den Gleichungen (2) entstehen, indem man darin für p, q, q', q'' je eine Auflösung der Gleichungen von der Form (6) setzt, deren p durch Δ_0 theilbar ist und welche, falls $\lambda = 2$ ist, aus ungeraden Zahlen besteht, mit T aber die Transformationen, welche den sämmtlichen Lösungen der Gleichung (11) sowie den nach oben gegebener Regel jedesmal zulässigen Lösungen der Gleichung (11a) entsprechen, so zerfallen alle möglichen ganzzahligen Transformationen der Form f in sich selbst in die verschiedenen Complexe

$$T \cdot S_0, \quad T \cdot S_1, \quad T \cdot S_2, \cdots$$

Z. B. nehmen die Transformationen der Form

$$f = \begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$$

mit der Adjungirten

$$F = \begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$$

oder auch die Transformationen der Form $x^2 + x'^2 - x''^2$ in sich selbst die Gestalt an:

$$(p^2 - q^2 - q'^2 + q''^2) \cdot x$$
$$= (p^2 - q^2 + q'^2 - q''^2)y + 2(pq'' - qq')y' + 2(pq' - qq'')y''$$
$$(p^2 - q^2 - q'^2 + q''^2) \cdot x'$$
$$= -2(pq'' + qq')y + (p^2 + q^2 - q'^2 - q''^2)y' - 2(pq + q'q'')y''$$
$$(p^2 - q^2 - q'^2 + q''^2) \cdot x''$$
$$= 2(pq' + qq'')y - 2(pq - q'q'')y' + (p^2 + q^2 + q'^2 + q''^2)y'',$$

während es nur die folgenden vier Gleichungen von der Form (6) giebt:

$$p^2 - q^2 - q'^2 + q''^2 = 1 \tag{15a}$$
$$p^2 - q^2 - q'^2 + q''^2 = 2 \tag{15b}$$
$$p^2 - q^2 - q'^2 + q''^2 = -1 \tag{15c}$$
$$p^2 - q^2 - q'^2 + q''^2 = -2. \tag{15d}$$

Der Lösung $p = 1$, $q = q' = 0$, $q'' = 1$ der zweiten entspricht die singuläre Transformation

$$S_1 = \begin{pmatrix} 0, & 1, & 0 \\ -1, & 0, & 0 \\ 0, & 0, & 1 \end{pmatrix}.$$

Bemerkt man ferner, dass aus einer Lösung p, q, q', q'' der Gleichung (15c) oder (15d) sogleich eine Lösung der Gleichung (15a) resp. (15b) entsteht, wenn man p mit q und q' mit q'' vertauscht, und umgekehrt, so findet man leicht, dass die entsprechenden Transformationen S' und S durch die Gleichung

$$S' = \begin{pmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 0, & -1 \end{pmatrix} \cdot S$$

mit einander verbunden sind; setzt man demnach

$$S_0 = \begin{pmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 0, & -1 \end{pmatrix},$$

so erhält man alle ganzzahligen Transformationen der Form

$$x^2 + x'^2 - x''^2$$

in sich selbst mittels der Formeln:

$$T, \quad T \cdot S_0, \quad T \cdot S_1, \quad T \cdot S_0 \cdot S_1.$$

Die hier mitgetheilten Sätze sind zuerst vom Verfasser gegeben worden (im Journ. f. d. r. u. a. Math. 71 S. 303). Bei Gauss findet sich für diesen Theil der Lehre von den ternären quadratischen Formen nur eine einzige kurze Notiz (aus seinem Nachlasse veröffentlicht im 2. Bd. seiner Werke S. 311), nach welcher die Transformationen der Form $x^2 + x'^2 - x''^2$ in sich selbst durch das Schema

$$\begin{array}{lll} \alpha\delta + \beta\gamma, & \alpha\beta - \gamma\delta, & \alpha\beta + \gamma\delta \\ \alpha\gamma - \beta\delta, & \frac{1}{2}(\alpha^2 + \delta^2 - \beta^2 - \gamma^2), & \frac{1}{2}(\alpha^2 + \gamma^2 - \beta^2 - \delta^2) \\ \alpha\gamma + \beta\delta, & \frac{1}{2}(\alpha^2 + \beta^2 - \gamma^2 - \delta^2), & \frac{1}{2}(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \end{array}$$

gegeben werden, wenn darin für $\alpha, \beta, \gamma, \delta$ die ganzzahligen Lösungen der Gleichung $\alpha\delta - \beta\gamma = 1$ in zwei geraden und zwei ungeraden Zahlen, sowie die ungeraden Vielfachen von $\sqrt{\frac{1}{2}}$, welche jener Gleichung genügen, gesetzt werden. Man überzeugt sich unschwer, dass von diesen beiden Bestimmungen die erstere den Auflösungen der Gleichung (15a), die andere den Auflösungen der Gleichung (15b) entspricht; von diesen aber werden die den beiden anderen entsprechenden als nicht wesentlich verschieden angesehen.

6. Es bleibt nun die Frage, in welcher Weise die unendlich vielen Transformationen T, welche den Auflösungen der Gleichung (11) resp. (11a) entsprechen, unter einander zusammenhängen, und ob etwa alle diese Auflösungen und damit auch jene Transformationen, ähnlich wie in der Lehre von den binären Formen, nämlich bei der Auflösung der Pell'schen

Gleichung, deren Analogon die Gleichungen (11) und (11a) bilden, auf eine endliche Anzahl von fundamentalen zurückgeführt werden können. Diese Frage harrt aber einstweilen noch ihrer Beantwortung und nur zum Theil wird sie im dritten Abschnitte dieses Werkes erledigt werden. Hier sei jedoch noch auf einen wesentlichen Unterschied aufmerksam gemacht, der in dieser Hinsicht zwischen den binären und den ternären quadratischen Formen (und umsomehr denjenigen mit mehr als drei Variabeln) besteht: bei der Zusammensetzung der Transformationen ist hier nämlich im Allgemeinen die Reihenfolge derselben von Einfluss d. i. die Transformationen sind nicht vertauschbar. Dies erkennt man sogleich aus den Formeln (78) des ersten Capitels, welche dazu dienen, die Elemente der aus zwei Transformationen durch Zusammensetzung entstehenden Transformation zu bestimmen; in der That verwandeln sich in denselben durch Umkehrung der Reihenfolge der Transformationen die Ausdrücke

$$\frac{1}{2}\frac{\partial f}{\partial(q's''-q''s')},\quad \frac{1}{2}\frac{\partial f}{\partial(q''s-qs'')},\quad \frac{1}{2}\frac{\partial f}{\partial(qs'-q's)}$$

in die entgegengesetzten. Demgemäss werden zwei Transformationen dann und nur dann vertauschbar sein, wenn diese Ausdrücke den Werth Null haben, d. h. wenn

$$q's''-q''s'=q''s-qs''=qs'-q's=0$$

ist. Dies geschieht erstens, wenn $q=q'=q''=0$ also eine der beiden Transformationen die identische ist, wo dann die Vertauschbarkeit beider selbstverständlich ist; zweitens, wenn

$$q:q':q''=s:s':s''$$

ist. Da nun bei ganzzahligen Transformationen die Elemente p, q, q', q'' als ganze Zahlen gedacht werden dürfen, werden die Elemente q, q', q'' aller unter einander vertauschbaren Transformationen Σ von der Form

$$q=z\cdot\gamma,\quad q'=z\cdot\gamma',\quad q''=z\cdot\gamma''$$

sein, in welcher $\gamma, \gamma', \gamma''$ drei ganze Zahlen ohne gemeinsamen Theiler, z aber eine ganze Zahl bedeutet.

Um diese vertauschbaren Transformationen Σ genauer zu untersuchen, verfahren wir wie Hermite*). Offenbar hat man die Zahlen $\gamma, \gamma', \gamma''$ dabei so anzunehmen, dass $F(\gamma, \gamma', \gamma'')$ Null oder negativ ist. Wir verfolgen hier nur den Fall, wo $F(\gamma, \gamma', \gamma'') < 0$ und prim zu 2Δ ist. Seien dann $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ ganze Zahlen von der Beschaffenheit, dass die Determinante

$$\begin{vmatrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{vmatrix} = 1$$

ist. Setzt man

$$\begin{aligned} y &= \alpha x + \alpha' x' + \alpha'' x'' \\ y' &= \beta x + \beta' x' + \beta'' x'' \\ y'' &= \gamma x + \gamma' x' + \gamma'' x'' \end{aligned}$$

und bezeichnet diese Beziehungen als die Substitution S, so verwandelt sich die Form $f(x, x', x'')$ durch die Substitution S^{-1} in eine äquivalente Form

$$f_1(y, y', y'') = \begin{pmatrix} a_1, & a_1', & a_1'' \\ b_1, & b_1', & b_1'' \end{pmatrix}$$

mit der Adjungirten

$$F_1 = \begin{pmatrix} A_1, & A_1', & A_1'' \\ B_1, & B_1', & B_1'' \end{pmatrix},$$

und da f durch die Substitution Σ in sich selbst übergeht, wird f_1 durch jede Substitution von der Form

(16) $$T = S \cdot \Sigma \cdot S^{-1}$$

ebenfalls in sich selbst übergehen. Zwischen den Variabeln x, x', x'' der Form f und den Variabeln X, X', X'', in welche die Substitution Σ die letzteren überführt, besteht aber die Gleichung (68) des ersten Capitels d. h. die Beziehung

(17) $$\gamma x + \gamma' x' + \gamma'' x'' = \gamma X + \gamma' X' + \gamma'' X''.$$

Wird demnach

$$\begin{aligned} \alpha X + \alpha' X' + \alpha'' X'' &= Y \\ \beta X + \beta' X' + \beta'' X'' &= Y' \\ \gamma X + \gamma' X' + \gamma'' X'' &= Y'' \end{aligned}$$

*) S. Journ. f. d. r. u. a. Math. 47, sur la théorie des formes quadratiques, I. mémoire.

gesetzt, so führt die zusammengesetzte Substitution (16) die Variabeln y in die Y über, und somit hat wegen (17) die Transformation T der Form f_1 in sich selbst die besondere Eigenthümlichkeit, dass bei ihr $y'' = Y''$ ist, die dritte Variable nämlich ungeändert bleibt.

Sei nun

$$(18) \qquad \begin{cases} y = \lambda Y + \mu Y' + \nu Y'' \\ y' = \lambda' Y + \mu' Y' + \nu' Y'' \\ y'' = \qquad\qquad\qquad\quad Y'' \end{cases}$$

irgend eine solche Substitution; dann ist

$$y = \lambda Y + \mu Y', \quad y' = \lambda' Y + \mu' Y'$$

offenbar eine Substitution, durch welche die binäre Form

$$(a_1, \ b_1'', \ a_1')$$

in sich selbst übergeht. Die Determinante $-A_1''$ der letzteren wird nach der Substitution S leicht dem Werthe $-F(\gamma, \gamma', \gamma'')$ gleich also positiv befunden. Die binäre Form selbst aber ist eigentlich durch f_1 und folglich auch durch f darstellbar und deshalb (s. die Bedingungen der Darstellbarkeit in nr. 3 vorigen Capitels) primitiv. Wenn folglich σ gleich 1 oder 2, je nachdem sie eigentlich oder uneigentlich primitiv ist, so muss

$$(19) \quad \lambda = \frac{\tau - b_1''v}{\sigma}, \quad \mu = \frac{-a_1'v}{\sigma}, \quad \lambda' = \frac{a_1 v}{\sigma}, \quad \mu' = \frac{\tau + b_1''v}{\sigma}$$

sein, wenn unter τ, v eine Lösung der Gleichung

$$(20) \qquad \tau^2 + A_1''v^2 = \sigma^2$$

verstanden wird. Die Substitution (18) liefert aber noch die anderen Bedingungsgleichungen:

$$(21) \begin{cases} a_1\nu^2 + a_1'\nu'^2 + 2b_1\nu' + 2b_1'\nu + 2b_1''\nu\nu' = 0 \\ a_1\lambda\nu + a_1'\lambda'\nu' + b_1\lambda' + b_1'\lambda + b_1''(\lambda\nu' + \lambda'\nu) = b_1' \\ a_1\mu\nu + a_1'\mu'\nu' + b_1\mu' + b_1'\mu + b_1''(\mu\nu' + \mu'\nu) = b_1, \end{cases}$$

aus deren beiden letzten man mittels der Werthe (19) zur Bestimmung von ν und ν' folgende Formeln erschliesst:

$$(22) \qquad \begin{cases} \sigma \cdot \nu = -B_1' \cdot \dfrac{\tau - \sigma}{A_1''} - b_1 v \\ \sigma \cdot \nu' = -B_1 \cdot \dfrac{\tau - \sigma}{A_1''} + b_1' v. \end{cases}$$

Wir bezeichnen mit d den grössten gemeinsamen Theiler von B_1', B_1, A_1'' und setzen $A_1'' = d \cdot \mathfrak{a}$. Damit die vorstehenden Formeln ganzzahlige Werthe liefern für v und v', ist nothwendig und zugleich auch ausreichend, dass $\tau \equiv \sigma \pmod{\mathfrak{a}}$ sei. Letzteres leuchtet für $\sigma = 1$ von selber ein; wenn aber $\sigma = 2$ ist, werden a_1, a_1' gerade, b_1'' und A_1'' also auch d und $\mathfrak{a}$ ungerade sein; wären alsdann b_1, b_1' und somit auch B_1', B_1 gerade, so würden die Bestandtheile zur Rechten der Formeln (22) gerade sein; wäre aber z. B. b_1 und folglich auch B_1' ungerade, so würden doch, da zufolge (20) die Zahlen τ, v und $\tau - \sigma$ und v gleichartige Zahlen sind, die beiden Bestandtheile des Ausdrucks für $\sigma \cdot v$ gleichartige Zahlen, der ganze Ausdruck also wieder gerade sein. Kurz: die nothwendige und hinreichende Bedingung dafür, dass v, v' ganzzahlig werden, ist die Bedingung $\tau \equiv \sigma \pmod{\mathfrak{a}}$.

Sei jetzt unter allen Auflösungen τ, v der Gleichung (20), deren $\tau \equiv \sigma \pmod{\mathfrak{a}}$ ist, T, U diejenige Auflösung, welche, ausgedrückt durch die Fundamentalauflösung T, U dieser Gleichung:

$$\frac{\mathsf{T} + \mathsf{U}\sqrt{-A_1''}}{\sigma} = \pm\left(\frac{T + U\sqrt{-A_1''}}{\sigma}\right)^n,$$

den kleinsten positiven Exponenten hat. Ist dann τ, v irgend eine andere Auflösung derselben Gleichung, bei welcher $\tau \equiv \sigma \pmod{\mathfrak{a}}$ ist, und

$$\frac{\tau + v\sqrt{-A_1''}}{\sigma} = \pm\left(\frac{T + U\sqrt{-A_1''}}{\sigma}\right)^m,$$

so kann man $m = hn + r$ setzen, wo h eine positive oder negative ganze Zahl und $0 \overline{\gtrless} r < n$ ist, und kann die vorige Gleichung folgendermassen schreiben:

$$\frac{\tau + v\sqrt{-A_1''}}{\sigma} \cdot \left(\frac{\mathsf{T} - \mathsf{U}\sqrt{-A_1''}}{\sigma}\right)^h = \pm\left(\frac{T + U\sqrt{-A_1''}}{\sigma}\right)^r,$$

wo man nun der linken Seite, wie leicht zu erkennen, die Gestalt

$$\frac{\tau' + v'\sqrt{-A_1''}}{\sigma}$$

geben kann, in welcher $\tau' \equiv \sigma \pmod{\mathfrak{a}}$; dies widerstreitet aber, da $r < n$, offenbar der Bedeutung der Zeichen T, U, aus-

genommen, wenn die rechte Seite gleich 1 ist, und somit findet man das Resultat: Jede Auflösung τ, v der Gleichung (20), bei welcher $\tau \equiv \sigma$ (mod. $\mathfrak{a}$), findet man aus der Auflösung T, U mittels der Formel:

$$\frac{\tau + v\sqrt{-A_1''}}{\sigma} = \left(\frac{\mathsf{T} + \mathsf{U}\sqrt{-A_1''}}{\sigma}\right)^h, \tag{23}$$

indem man für h sämmtliche (positive oder negative) ganze Zahlen setzt.

Und demnach findet man sämmtliche Transformationen (18) der Form f_1 in sich selbst, wenn man in den Gleichungen (19) und (22) die Zahlen τ, v der Gleichung (23) gemäss wählt; die so erhaltenen Substitutionen (18) sind aber auch wirklich Transformationen der gedachten Art, da die entsprechenden Werthe ν, ν' auch der ersten der Gleichungen (21) genügen.

Man schreibe hiernach die Substitution (18), wie folgt:

$$\begin{aligned}
\sigma \cdot y &= \tau \cdot Y - B_1' \cdot \frac{\tau - \sigma}{A_1''} \cdot Y'' - (b_1''Y + a_1'Y' + b_1Y'') \cdot v \\
\sigma \cdot y' &= \tau \cdot Y' - B_1 \cdot \frac{\tau - \sigma}{A_1''} \cdot Y'' + (a_1Y + b_1''Y' + b_1'Y'') \cdot v \\
\sigma \cdot y'' &= \sigma \cdot Y'',
\end{aligned}$$

dann findet man leicht die Gleichungen

$$\begin{aligned}
&\sigma \cdot (b_1''y + a_1'y' + b_1y'') \\
&= (b_1''Y + a_1'Y' + b_1Y'')\tau + (A_1''Y - B_1'Y'')v \\
&\sigma \cdot (A_1''y - B_1'y'') \\
&= (A_1''Y - B_1'Y'')\tau - (b_1''Y + a_1'Y' + b_1Y'')A_1''v
\end{aligned}$$

und hieraus folgende Beziehung:

$$\begin{aligned}
&A_1''y - B_1'y'' + (b_1''y + a_1'y' + b_1y'')\sqrt{-A_1''} \\
&= \frac{\tau + v\sqrt{-A_1''}}{\sigma} \cdot \\
&\cdot (A_1''Y - B_1'Y'' + (b_1''Y + a_1'Y' + b_1Y'')\sqrt{-A_1''})
\end{aligned}$$

d. i. wegen (23)

$$\begin{aligned}
&= \left(\frac{\mathsf{T} + \mathsf{U}\sqrt{-A_1''}}{\sigma}\right)^h \cdot \\
&\cdot (A_1''Y - B_1'Y'' + (b_1''Y + a_1'Y' + b_1Y'')\sqrt{-A_1''}),
\end{aligned}$$

eine Beziehung, welche zusammen mit der Gleichung

$$y'' = Y''$$

die Formeln (18) vertritt. Bezeichnet man nun mit T_1 die auf solche Weise für $h = 1$ definirte Substitution (18), so ist offenbar die einem beliebigen Exponenten h entsprechende Substitution (18) gleich T_1^h. Da aber jede der Transformationen (16) eine der Transformationen (18) ist (und umgekehrt), so ergiebt sich hiernach

$$T = S \cdot \Sigma \cdot S^{-1} = T_1^h$$

also auch

$$\Sigma = S^{-1} \cdot T_1^h \cdot S = (S^{-1} \cdot T_1 \cdot S)^h$$

und folglich der Hermite'sche Satz: Alle unter einander vertauschbaren Transformationen einer (eigentlich primitiven) ternären quadratischen Form in sich selbst (der angegebenen Art) sind Potenzen oder Wiederholungen einer einzigen von ihnen.

Fünftes Capitel.

Vom Vorhandensein der Geschlechter.

a) Die binären Formen.

1. Die Congruenzbedingung (20) des dritten Capitels, welche erfüllbar sein muss, wenn eine binäre quadratische Form φ durch eine ternäre Form von der Ordnung (Ω, Δ) eigentlich darstellbar sein soll, verknüpft die Theorie der ternären Formen mit demjenigen Theile der Lehre von den binären, welcher von ihren Geschlechtern handelt. Wir sind dadurch genöthigt, diesen Abschnitt der genannten Lehre so weit hier darzustellen, als es für unsern Zweck erforderlich ist, beziehen uns jedoch dabei zur Abkürzung wie zur Ergänzung auf den gleichnamigen 9. Abschnitt unserer Darstellung der analytischen Zahlentheorie (Leipzig, bei B. G. Teubner, 1894).

Sei

$$ax^2 + 2bxy + cy^2$$

eine primitive (positive) binäre quadratische Form, ihre Deter-

minante $D = b^2 - ac$ von Null und von einer positiven Quadratzahl verschieden. Ganz wie bei ternären quadratischen Formen überzeugt man sich, dass durch eine eigentlich-primitive Form Zahlen dargestellt werden können, welche zu einer beliebig gegebenen Zahl prim sind, durch eine uneigentlich-primitive Form wenigstens das Doppelte solcher Zahlen. Setzt man also $\sigma = 1$ oder 2, jenachdem die Form eigentlich- oder uneigentlich-primitiv ist, so kann

$$f = \frac{ax^2 + 2bxy + cy^2}{\sigma}$$

zu jeder beliebig gegebenen Zahl prim gemacht werden. Wir wählen hier $2D$ zu dieser Zahl. Sind dann m', m'' irgend zwei solche Werthe von f:

$$m' = \frac{a\alpha'^2 + 2b\alpha'\gamma' + c\gamma'^2}{\sigma}, \quad m'' = \frac{a\alpha''^2 + 2b\alpha''\gamma'' + c\gamma''^2}{\sigma},$$

so folgt auf Grund der fundamentalen Gleichung

$$(1) \quad \begin{cases} (a\alpha'^2 + 2b\alpha'\gamma' + c\gamma'^2) \cdot (a\alpha''^2 + 2b\alpha''\gamma'' + c\gamma''^2) \\ = (a\alpha'\alpha'' + b(\alpha'\gamma'' + \alpha''\gamma') + c\gamma'\gamma'')^2 - D(\alpha'\gamma'' - \alpha''\gamma')^2 \end{cases}$$

und wenn man

$$a\alpha'\alpha'' + b(\alpha'\gamma'' + \alpha''\gamma') + c\gamma'\gamma'' = x, \quad \alpha'\gamma'' - \alpha''\gamma' = y$$

setzt,

$$(2) \qquad \sigma m' \cdot \sigma m'' = x^2 - Dy^2.$$

Sei nun zuerst $\sigma = 1$.

Für jede ungerade in D aufgehende Primzahl q folgt hieraus

$$\left(\frac{m'}{q}\right) = \left(\frac{m''}{q}\right)$$

d. h. für alle zu $2D$ primen Werthe von f hat das Symbol $\left(\frac{f}{q}\right)$ ein- und denselben Werth.

Ist $D \equiv 3 \pmod{4}$, so folgt aus (2)

$$m' \cdot m'' \equiv 1 \pmod{4}$$

also hat für alle jene Werthe das Symbol $(-1)^{\frac{f-1}{2}}$ gleichen Werth.

Ist $D \equiv 2 \pmod{8}$, so ergiebt sich aus (2)

$$m' \cdot m'' \equiv x^2 - 2y^2 \pmod{8}$$

und daraus leicht, dass für alle jene Werthe das Symbol $(-1)^{\frac{f^2-1}{8}}$ gleichen Werth hat.

Für $D \equiv 6 \pmod{8}$ folgt ebenso, dass für alle gedachten Werthe von f das Symbol

$$(-1)^{\frac{f-1}{2}+\frac{f^2-1}{8}}$$

gleichen Werth hat.

Für $D \equiv 4 \pmod{8}$ folgt wieder für alle jene Werthe von f derselbe Werth des Symbols $(-1)^{\frac{f-1}{2}}$.

Endlich für $D \equiv 0 \pmod{8}$ folgt $m' \cdot m'' \equiv 1 \pmod{8}$, also hat dann für alle jene Werthe von f jedes der Symbole $(-1)^{\frac{f-1}{2}}$ und $(-1)^{\frac{f^2-1}{8}}$ je ein- und denselben Werth.

Ist zweitens $\sigma = 2$ also a, c gerade, dagegen b ungerade, so muss $D = b^2 - ac$ congruent 1 (mod. 4) sein. Ist dann q irgend eine in D aufgehende Primzahl, so folgt aus (2)

$$\left(\frac{2m'}{q}\right) \cdot \left(\frac{2m''}{q}\right) = \left(\frac{m'}{q}\right) \cdot \left(\frac{m''}{q}\right) = 1$$

also hat für die sämmtlichen zu $2D$ primen Werthe von f das Symbol $\left(\frac{f}{q}\right)$ ein- und denselben Werth.

Hiernach giebt es also für jede Determinante und jede zu ihr gehörige eigentlich- oder uneigentlich-primitive binäre quadratische Form gewisse Einheiten, welche für die sämmtlichen mit f bezeichneten Zahlen ein- und denselben Werth haben. Diese, der betrachteten Form eigenthümlichen Werthe können als besondere Charaktere der Form bezeichnet werden. Ihre Anzahl ist, wie aus der vorstehenden Uebersicht hervorgeht, $\varpi + \lambda$, wenn ϖ die Anzahl der verschiedenen ungeraden Primfaktoren bedeutet, aus denen D besteht, und für eigentlich-primitive Formen

so oft $D \equiv 1 \pmod{4}$, $\lambda = 0$

" " $D \equiv 2, 3, 4, 6, 7 \pmod{8}$, $\lambda = 1$

" " $D \equiv 0 \pmod{8}$, $\lambda = 2$

für uneigentlich primitive Formen $\lambda = 0$

ist.

Die Gesammtheit aller einer Form zukommenden

Einzelcharaktere d. i. die Werthe der ihr entsprechenden in der Uebersicht angeführten Symbole bildet den Gesammtcharakter der Form. Da jeder der Einzelcharaktere sowohl den Werth $+1$ als -1 haben kann, wird die Anzahl der an sich denkbaren Gesammtcharaktere gleich der Anzahl der Combinationen dieser Werthe d. i. gleich $2^{\omega+\lambda}$ sein.

Da durch äquivalente Formen stets dieselben Zahlen darstellbar sind, leuchtet ein, dass der Gesammtcharakter einer Form immer auch der Gesammtcharakter jeder ihr äquivalenten Form oder auch derjenige ihrer Classe ist. Alle Classen von binären Formen derselben Determinante nun, welche übereinstimmenden Gesammtcharakter haben, nennt man ein Geschlecht binärer Formen. Die Anzahl der verschiedenen Geschlechter ist also gewiss nicht grösser, als die der angebbaren Gesammtcharaktere; ob sie ihr aber gleich, oder geringer als sie, suchen die folgenden Betrachtungen festzustellen. Dabei beschränken wir uns aber auf eigentlich-primitive Formen.

2. Das hierzu anzuwendende Hilfsmittel ist die Lehre von der Zusammensetzung binärer quadratischer Formen*). Dieser Lehre gemäss lassen sich, wenn C und C' — wo auch C' identisch sein darf mit C — irgend zwei Classen solcher Formen mit der Determinante D sind, in denselben stets Formen F und F' so auswählen, dass ihr Produkt wieder eine Form F'' der nämlichen Determinante D ist, und die Classe C'', zu welcher die letztere gehört, erweist sich als unabhängig von jener Auswahl, die auf mannigfaltigste Weise möglich ist, allein bestimmt von den gegebenen Classen C und C'. Die so definirte Classe C'' heisst aus C und C' zusammengesetzt oder ihr Produkt, in Zeichen:

$$C'' = C \cdot C'.$$

Ist hierbei eine der Classen C, C' gleich der Hauptclasse H, d. i. derjenigen Classe, welche die Hauptform $x^2 - Dy^2$ enthält, so ist die zusammengesetzte Classe C'' gleich der andern:

$$H \cdot C = C \cdot H = C. \tag{3}$$

---

*) S. darüber des Verfassers Elemente der Zahlentheorie S. 240 u. ff.

Von dieser Grundlage aus kann man zeigen, dass es für jede Classe C von Formen mit der Determinante D einen kleinsten Exponenten m der Art giebt, dass C^m mit der Hauptclasse H identisch wird; dieser Exponent heisst der Exponent, zu welchem die Classe C gehört. Und ferner lässt sich zeigen, dass jede Classe C auf eine einzige Weise mittels gewisser Fundamentalclassen $C_1, C_2, \ldots C_\omega$ durch die Formel

$$(4) \qquad C = C_1^{h_1} \cdot C_2^{h_2} \ldots C_\omega^{h_\omega}$$

ausgedrückt werden kann, wenn darin für $h_1, h_2, \ldots h_\omega$ alle ganzen Zahlen gesetzt werden, welche resp. nicht grösser sind als die Exponenten $m_1, m_2, \ldots m_\omega$, zu denen die Fundamentalclassen gehören.

Eine Classe, die aus einer anderen C hervorgeht, wenn letztere mit sich selbst zusammengesetzt wird, heisst die durch Duplikation von C entstandene Classe.

Entsteht durch Duplikation einer Classe C die Hauptclasse:

$$C \cdot C = H,$$

so nennt man C eine ambige Classe. Eine Classe C', welche mit C zusammengesetzt die Hauptclasse H hervorbringt, heisst aber allgemein die zu C entgegengesetzte Classe. Demnach darf man die ambigen Classen auch als diejenigen definiren, die mit ihrer entgegengesetzten Classe identisch sind. Die Formel (4) lässt unschwer erkennen, dass die Anzahl aller ambigen Classen gleich 2^μ ist, wenn μ von den Exponenten $m_1, m_2, \ldots m_\omega$ gerade sind.

Bezeichnet man nun mit $\varphi(f)$ jedes der Symbole

$$\left(\frac{f}{q}\right), \quad (-1)^{\frac{f-1}{2}}, \quad (-1)^{\frac{f^2-1}{8}}, \quad (-1)^{\frac{f-1}{2}+\frac{f^2-1}{8}},$$

deren Werthe den Gesammtcharakter einer Form oder Classe bestimmen, so leistet die so definirte Funktion ersichtlich der Gleichung Genüge:

$$(5) \qquad \varphi(m') \cdot \varphi(m'') = \varphi(m'm'').$$

Sind aber m', m'' durch je eine Form der Classe C und C' darstellbar, so ist es $m'm''$ durch eine Form der Classe

$$C \cdot C' = C''.$$

Demzufolge ergiebt sich aus den Gesammtcharakteren zweier Classen C und C' auf ganz bestimmte Weise der Gesammtcharakter der aus ihnen zusammengesetzten Classe.

Für die Hauptclasse H werden aber sämmtliche Einzelcharaktere $+1$ sein, denn die Hauptclasse enthält die Hauptform $x^2 - Dy^2$, durch welche die Zahl $f = 1$ dargestellt wird. Versteht man also unter Hauptgeschlecht dasjenige Geschlecht, welchem die Hauptclasse angehört, so hat auch für jede Classe des Hauptgeschlechts jeder Einzelcharakter den Werth $+1$. Mithin bleiben, wenn man irgend eine Classe C mit einer Classe des Hauptgeschlechts zusammensetzt, nach Gleichung (5) die Einzelcharaktere der Classe C auch die der zusammengesetzten Classe, mit andern Worten: wird eine Classe C mit einer Classe des Hauptgeschlechtes zusammengesetzt, so gehört die zusammengesetzte Classe demselben Geschlechte an, wie C.

Aus (5) folgt ferner, dass aus der Zusammensetzung zweier Classen, deren Einzelcharaktere übereinstimmen, eine Classe entsteht, deren Einzelcharaktere sämmtlich $+1$ sind, d. h.: die Classe, welche aus zwei Classen gleichen Geschlechtes zusammengesetzt ist, gehört zum Hauptgeschlechte. Insbesondere gehört demnach jede Classe, welche durch Duplikation entsteht, dem Hauptgeschlecht an.

Der erste dieser beiden Sätze darf offenbar auch umgekehrt werden, und daraus folgt u. A., dass die Classe, welche einer anderen entgegengesetzt ist, demselben Geschlechte angehört, wie diese. Auch schliesst man, dass der Exponent m, zu welchem eine Classe C gehört, stets gerade ist, so oft C nicht eine Classe des Hauptgeschlechts ist*).

Auf Grund dieser Sätze zeigt man ferner leicht, dass jedes Geschlecht gleichviel Classen enthält**). Nennt man demnach $H(D)$ die Anzahl aller Classen eigentlich-primi-

*) S. analytische Zahlentheorie S. 251.

**) Ebendas. S. 251.

tiver Formen mit der Determinante D, $K(D)$ die Anzahl dieser Formenclassen im Hauptgeschlechte, und $G(D)$ die Anzahl der Geschlechter, so geht unmittelbar die Gleichung

(6) $$H(D) = K(D) \cdot G(D)$$

hervor. Eine zweite, ähnliche Formel für $H(D)$ gewinnt man aus der Betrachtung der Classen, welche durch Duplikation entstehen. Bedeutet nämlich $\mathfrak{A}(D)$ die Anzahl der ambigen Classen, $Q(D)$ die Anzahl der Classen, welche durch Duplikation entstehen, so findet die Beziehung statt*):

(7) $$H(D) = \mathfrak{A}(D) \cdot Q(D).$$

Vermittelst der Formel (4) kann man sich aber leicht überzeugen, dass

(8) $$G(D) \gtreqless \mathfrak{A}(D)$$

ist. Wie schon bemerkt, ist $\mathfrak{A}(D) = 2^\mu$, wenn μ von den Exponenten $m_1, m_2, \ldots m_\omega$ gerade sind; gehören aber γ von den Fundamentalclassen nicht dem Hauptgeschlechte an, so sind deren Exponenten, wie auch schon angeführt, jedenfalls gerade, also ist $\mu \geqq \gamma$ und $2^\mu \geqq 2^\gamma$. Sei g die Anzahl der verschiedenen Geschlechter $\Gamma_1, \Gamma_2, \ldots$, in welche diese γ Fundamentalclassen sich vertheilen, so wird $\gamma \geqq g$ also $2^\gamma \geqq 2^g$ sein. Nun entsteht durch Zusammensetzung von Classen des Hauptgeschlechts unter einander stets wieder eine solche; durch Zusammensetzung von Classen eines vom Hauptgeschlechte verschiedenen Geschlechts Γ, sei es unter einander, sei es mit Classen des Hauptgeschlechts, stets wieder eine Classe des letzteren oder des Geschlechts Γ; und folglich kann die Anzahl der verschiedenen Geschlechter, welche durch Zusammensetzung aus den Fundamentalclassen entstehen können, d. i. die Anzahl sämmtlicher Geschlechter nicht grösser sein, als die Anzahl der Glieder des entwickelten Produkts:

$$(1 + \Gamma_1)(1 + \Gamma_2) \cdots (1 + \Gamma_g)$$

d. h.

$$2^g \geqq G(D).$$

Alle diese Ungleichheiten zusammengenommen bestätigen aber die Formel (8) oder den Satz: Die Anzahl aller *wirklich*

---

*) S. analytische Zahlentheorie S. 255.

vorhandenen Geschlechter ist höchstens gleich der Anzahl aller ambigen Classen.

Diese letztere Anzahl lässt sich nun, wie Gauss in den art. 257—259 der Disquis. Arithm. gezeigt hat, ohne andere Hilfsmittel als die von ihm definirten reducirten Formen und die Sätze über ihre Aequivalenz allgemein bestimmen; hier müssen wir uns damit begnügen, den Leser auf seine Herleitung zu verweisen; es findet sich so, dass die Anzahl der ambigen Classen stets halb so gross ist, als die Anzahl aller angebbaren Gesammtcharaktere. Gemäss der Formel (8) aber ist dann zu schliessen, dass der einen Hälfte dieser Gesammtcharaktere keine Geschlechter binärer Formen mit der Determinante D wirklich entsprechen.

3. Eine Anwendung dieses Resultates auf gewisse einfache Fälle giebt Gauss die Grundlage für seinen zweiten Beweis des quadratischen Reciprocitätsgesetzes. Bei der Bedeutung dieses Gesetzes sowie des bezüglichen Gaussschen, von seinen übrigen grundverschiedenen Beweises desselben ist es wünschenswerth, nichts unbewiesen zu lassen und deshalb nicht auf die Gauss'sche allgemeine Bestimmung der Anzahl der ambigen Classen zurückzugreifen. Es soll diese Anzahl vielmehr für die in Frage kommenden besonderen Fälle direkt ermittelt werden, wo dann der Beweis, auf die Formel (8) gestützt, sich folgendermassen gestaltet.

Vorweg sei daran erinnert*), dass in jeder ambigen Classe auch eine ambige Form d. i. eine Form (a, b, c) sich befindet, in welcher $2b \equiv 0 \pmod{a}$ ist, andererseits eine solche Form auch nur in einer ambigen Classe enthalten sein kann.

Demnach wird man alle ambigen Classen repräsentiren, wenn man sämmtliche nicht äquivalente ambige Formen aufstellt. Wegen

$$2b^2 - 2ac = 2D$$

muss aber bei letzteren a nothwendig ein Theiler von $2D$ sein, und da (a, B, C) mit (a, b, c) äquivalent ist, so oft bei gleicher Determinante

*) S. El. d. Zahlenth. S. 235.

$$B \equiv b \pmod{a}$$

ist, darf man sich von vornherein auf solche (eigentlich-primitive) Formen beschränken, bei welchen $b < a$ also entweder $b = 0$ oder $b = \pm \frac{a}{2}$ ist.

Man bemerke ferner, dass, weil es für jede Determinante D wenigstens eine Form, die Hauptform $x^2 - Dy^2$ giebt, auch die Anzahl der Classen sowie die der Geschlechter mindestens gleich 1 sein muss.

Dies vorausgeschickt, betrachte man nun folgende einfache Fälle:

1) Ist $D = -1$, so giebt es überhaupt nur eine Classe, die durch die Hauptform $x^2 + y^2$ repräsentirte Hauptclasse*), welche stets ambige ist, also giebt es, wie nur eine ambige Classe, so auch nur ein Geschlecht, das Hauptgeschlecht. Nach der Uebersicht in nr. 1 ist der einzige für diese Determinante vorhandene Einzelcharakter $(-1)^{\frac{f-1}{2}}$ und folglich für jede ungerade durch $x^2 + y^2$ darstellbare Zahl f

$$(-1)^{\frac{f-1}{2}} = 1. \tag{9}$$

2) Ist $D = +2$, so kann a nur einen der Werthe

$$\pm 1, \quad \pm 2, \quad \pm 4$$

haben; in Rücksicht auf die Bedingung $b^2 - ac = 2$ finden sich also nur folgende eigentlich-primitive Formen, die in Betracht kommen:

$$x^2 - 2y^2, \quad -x^2 + 2y^2, \quad 2x^2 - y^2, \quad -2x^2 + y^2.$$

Von ihnen gehören die erste und vierte, die zweite und dritte derselben Classe an; da aber die zweite in die erste durch die Substitution

$$x = x' - 2y', \quad y = x' - y'$$

übergeht, so giebt es auch in diesem Falle nur eine ambige Classe und ein einziges Geschlecht, nämlich das Hauptgeschlecht. Der einzige hier vorhandene Charakter ist $(-1)^{\frac{f^2-1}{8}}$ und dem-

*) El. der Zahlentheorie, S. 222.

nach ist für jede ungerade durch eine Form mit der Determinante 2 darstellbare Zahl f

(10) $$(-1)^{\frac{f^2-1}{8}} = 1.$$

3) Ist $D = \pm p \equiv 1 \pmod{4}$, während p eine Primzahl ist, so giebt es gleichfalls nur eine ambige Classe*), repräsentirt durch die Hauptform $x^2 \mp py^2$, also nach dem Satze, auf den wir uns stützen, auch nur ein Geschlecht, das Hauptgeschlecht. Der einzige in diesem Falle vorhandene Charakter, $\left(\frac{f}{p}\right)$, hat demnach für jede durch p nicht theilbare, durch die Formen mit der Determinante $\pm p$ darstellbare Zahl f den Werth

(11) $$\left(\frac{f}{p}\right) = +1.$$

Aus diesen Resultaten ist aber Folgendes zu erschliessen.

Zunächst gilt für jede ungerade Primzahl p die Gleichung

(12) $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

In der That, ist $(-1)^{\frac{p-1}{2}} = 1$, nämlich p von der Form $4n+1$, so ist $px^2 - y^2$ eine eigentlich-primitive Form mit der Determinante $D = p \equiv 1 \pmod{4}$, durch welche -1 darstellbar ist, also nach (11) auch $\left(\frac{-1}{p}\right) = +1$. Ist dagegen $(-1)^{\frac{p-1}{2}} = -1$, so muss auch $\left(\frac{-1}{p}\right) = -1$ sein, denn sonst wäre p durch die Form $x^2 + y^2$ mit der Determinante -1 darstellbar, also nach (9) $(-1)^{\frac{p-1}{2}} = +1$, gegen die Voraussetzung. Hiermit ist die Gleichung (12) für alle Fälle bewiesen.

Zweitens besteht für jede ungerade Primzahl p die Gleichung

(13) $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Ist nämlich zuerst $(-1)^{\frac{p^2-1}{8}} = +1$, so ist $p \equiv \pm 1$

*) El. der Zahlentheorie S. 259.

(mod. 8) oder $\pm p = 1 + 8h$ und, jenachdem dann h gerade oder ungerade ist, ist

$$\left(8,\ 3,\ \frac{9 \mp p}{8}\right) \quad \text{oder} \quad \left(8,\ 1,\ \frac{1 \mp p}{8}\right)$$

eine eigentlich-primitive Form der Determinante

$$D = \pm p \equiv 1 \pmod{4}$$

und, da 8 durch sie darstellbar ist, wegen (11)

$$\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right) = +1.$$

Ist aber $(-1)^{\frac{p^2-1}{8}} = -1$, so muss auch $\left(\frac{2}{p}\right) = -1$ sein, denn sonst wäre p darstellbar durch eine Form mit der Determinante 2 und folglich wegen (10)

$$(-1)^{\frac{p^2-1}{8}} = +1,$$

gegen die Voraussetzung.

Sind drittens p, q zwei von einander verschiedene ungerade Primzahlen, von denen wenigstens eine, etwa q, von der Form $4n + 1$ ist, so ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right). \tag{14}$$

Denn, ist zunächst $\left(\frac{p}{q}\right) = +1$, so ist nach (12) auch $\left(\frac{-p}{q}\right) = +1$. Man wähle also das Vorzeichen so, dass

$$\pm p \equiv 1 \pmod{4}$$

wird, dann wird q darstellbar sein durch eine Form mit der Determinante $D = \pm p \equiv 1 \pmod{4}$ und folglich ist wegen (11) $\left(\frac{q}{p}\right) = +1$. Ist aber umgekehrt $\left(\frac{p}{q}\right) = -1$, so muss auch $\left(\frac{q}{p}\right) = -1$ sein, denn sonst wäre p darstellbar durch eine Form mit der Determinante $D = q \equiv 1 \pmod{4}$ und folglich nach (11) gegen die Voraussetzung $\left(\frac{p}{q}\right) = +1$.

Sind dagegen p, q beides Primzahlen von der Form

$$4n + 3,$$

so bedarf es noch der Betrachtung eines neuen Falles, nämlich der Determinante $pq \equiv 1 \pmod{4}$. Um in diesem Falle

sämmtliche ambigen Classen zu finden, muss man für a die Werthe ± 1, ± 2, $\pm p$, $\pm 2p$, $\pm q$, $\pm 2q$, $\pm pq$, $\pm 2pq$ versuchen. Die geraden darf man aber sofort verwerfen, da, wenn a gerade, wegen $b^2 - ac = pq$ nothwendig b ungerade, dann aber c aus $-ac = pq - b^2 \equiv 0 \pmod{4}$ gerade, die Form (a, b, c) also nicht eigentlich-primitiv sein würde. Ist aber a ungerade, so wird $b = 0$ und es kommen daher nur folgende Formen in Betracht:

$$\begin{array}{llll} x^2 - pqy^2, & -x^2 + pqy^2, & px^2 - qy^2, & -px^2 + qy^2 \\ qx^2 - py^2, & -qx^2 + py^2, & pqx^2 - y^2, & -pqx^2 + y^2, \end{array}$$

von denen jedoch die vier letzten, weil den vier ersten in umgekehrter Reihenfolge äquivalent, wegzulassen sind. Nun ist die Gleichung

$$-x^2 + pqy^2 = 1$$

unmöglich, von den beiden Gleichungen

$$px^2 - qy^2 = 1, \quad -px^2 + qy^2 = 1$$

aber eine nothwendig auflösbar*), demnach ist eine der beiden Formen $px^2 - qy^2$, $-px^2 + qy^2$ der Form $x^2 - pqy^2$ und dann die andere der Form $-x^2 + pqy^2$ äquivalent, dagegen die beiden letztgenannten einander nicht äquivalent. Und sonach giebt es in diesem Falle zwei ambige Classen, also höchstens zwei verschiedene Geschlechter. Diese sind aber auch in der That vorhanden, denn der Hauptform $x^2 - pqy^2$ kommen die Einzelcharaktere

$$\left(\frac{f}{p}\right) = +1, \quad \left(\frac{f}{q}\right) = +1,$$

der Form $-x^2 + pqy^2$ aber, durch welche -1 darstellbar ist, die Charaktere

$$\left(\frac{f}{p}\right) = \left(\frac{-1}{p}\right) = -1, \quad \left(\frac{f}{q}\right) = \left(\frac{-1}{q}\right) = -1$$

zu. Demnach müssen die Charaktere der Form $px^2 - qy^2$ entweder mit den ersteren übereinstimmen, also

$$\left(\frac{f}{p}\right) = \left(\frac{-q}{p}\right) = 1, \quad \left(\frac{f}{q}\right) = \left(\frac{p}{q}\right) = 1, \quad \text{d. h.} \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

sein, oder sie müssen mit den letzteren identisch, also

---

*) El. der Zahlentheorie S. 256.

$$\left(\frac{f}{p}\right)=\left(\frac{-q}{p}\right)=-1,\quad \left(\frac{f}{q}\right)=\left(\frac{p}{q}\right)=-1$$

d. h. wieder

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$$

sein, und somit findet man den Satz:

Sind viertens p, q zwei Primzahlen von der Form $4n+3$, so ist

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right). \tag{15}$$

Die Formeln (14) und (15) fassen sich zusammen in die einzige Formel des Reciprocitätsgesetzes:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}, \tag{16}$$

welches damit bewiesen ist.

4. Aus den Formeln (12), (13), (16) erhält man nun bekanntlich allgemeiner

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}},\quad \left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}, \tag{17}$$

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}; \tag{18}$$

P bedeutet eine ungerade Zahl, die in der ersten Formel positiv sein muss; in der dritten sind P, Q zwei ungerade relativ-prime Zahlen, von denen wenigstens eine positiv sein muss, und die Symbole sind die verallgemeinerten Legendre-schen, die sogenannten Jacobi'schen Symbole. Diese Gleichungen führen unmittelbar zu einer Formel, welche von Dirichlet gegeben worden ist. Eine beliebige, nur von einem positiven Quadrate verschiedene ganze Zahl D kann stets in folgende Form gesetzt werden:

$$D=\pm 2^c\cdot P\cdot S^2, \tag{19}$$

wenn man unter S^2 das grösste in D aufgehende Quadrat, unter c also 0 oder 1, unter P eine aus lauter verschiedenen ungeraden Primfaktoren bestehende ganze Zahl versteht. Setzen wir $\delta=+1$, wenn $\pm P\equiv 1 \pmod 4$, dagegen $\delta=-1$, wenn $\pm P\equiv 3 \pmod 4$ ist, sodass immer $(-1)^{\frac{\pm P-1}{2}}=\delta$

wird, und setzen ferner $\varepsilon = \pm 1$, jenachdem c gleich 0 oder 1 ist, so folgt aus (19) gemäss den Gleichungen (17) und (18) für jede positive zu $2D$ prime Zahl f die Dirichlet'sche Formel

$$(20) \qquad \left(\frac{D}{f}\right) = \delta^{\frac{f-1}{2}} \cdot \varepsilon^{\frac{f^2-1}{8}} \cdot \left(\frac{f}{P}\right).$$

Ist nun f irgend eine positive zu $2D$ prime Zahl, welche durch eine Form der Determinante D eigentlich darstellbar ist, so muss bekanntlich $\left(\frac{D}{f}\right) = +1$ sein oder die Gleichung stattfinden:

$$(21) \qquad \delta^{\frac{f-1}{2}} \cdot \varepsilon^{\frac{f^2-1}{8}} \cdot \left(\frac{f}{P}\right) = 1.$$

Diese Gleichung, in welcher die linke Seite ein Produkt von Einzelcharakteren der bezüglichen Determinante ist, beschränkt offenbar die willkürliche Wahl aller vorhandenen Einzelcharaktere und ihre Combinationen in solcher Weise, dass nur die Hälfte aller Combinationen zulässig bleibt. Sie giebt also, unabhängig von der Gauss'schen Bestimmung der Anzahl ambiger Classen, den mit Hilfe dieser Bestimmung oben gefundenen Satz, dass der einen Hälfte der angebbaren Gesammtcharaktere keine Geschlechter binärer Formen wirklich entsprechen, zugleich aber dient sie dazu, diese Hälfte genau zu charakterisiren: derjenigen Hälfte der angebbaren Gesammtcharaktere nämlich, für welche die Gleichung (21) nicht erfüllt ist, entsprechen keine Geschlechter binärer Formen mit der Determinante D.

5. Es bleibt nunmehr zu erörtern, ob jedem Gesammtcharakter der anderen Hälfte, die hiernach allein noch zulässig bleibt, stets ein wirklich vorhandenes Geschlecht binärer Formen entspricht. Die Frage ist, wie sich zeigen wird, zu bejahen, und eben dieser Umstand wird es ermöglichen, die weitere Frage zu beantworten, ob auch die im zweiten Capitel definirten Geschlechter ternärer quadratischer Formen sämmtlich vorhanden sind.

Zu solchem Zwecke wenden wir die im dritten Capitel entwickelten Betrachtungen auf die ternären Formen der Ordnung $(-1, 1)$ an. Vorweg sei bemerkt, was erst an späterer

Stelle*) bewiesen werden kann, dass sämmtliche Formen dieser Ordnung nur eine einzige Classe bilden, welche repräsentirt werden kann durch die Form

$$(22) \qquad f_1 = -x^2 + 2x'x''.$$

Das in jenem Capitel mit (32) bezeichnete Formensystem reducirt sich demnach auf diese einzige Form f_1. Durch die Formen der gedachten Ordnung können aber nach den dortigen Auseinandersetzungen nur negative oder unbestimmte binäre Formen dargestellt werden, und eine solche Form φ mit der Determinante $D = -M''\Omega$ ist auch wirklich durch das Formensystem d. i. im vorliegenden Falle durch die Form f_1 eigentlich darstellbar, wenn für sie die dortige Congruenz (20), die hier wegen $\Omega = -1$, $\Delta = 1$ folgendermassen lautet:

$$(23) \qquad (Ny - N'y')^2 + \varphi \equiv 0 \pmod{D},$$

möglich ist. Nach (24) daselbst wird dies für eine Form

$$\varphi = my^2 + 2n''yy' + m'y'^2$$

der Fall sein, wenn die Form $(-m, \pm n'', -m')$ zum Hauptgeschlechte für die Determinante D gehört.

Sei also (μ, ν'', μ') eine binäre Form mit der Determinante D, welche zum Hauptgeschlechte gehört, also eine eigentlich-primitive und im Falle $D < 0$ eine positive Form, und

$$m = -\mu, \quad n'' = \nu'', \quad m' = -\mu',$$

so ist die Form φ d. i. die Form

$$(24) \qquad -\mu y^2 + 2\nu''yy' - \mu'y'^2$$

durch die Form (22) und folglich die Form

$$\mu y^2 - 2\nu''yy' + \mu'y'^2$$

durch die Form $x^2 - 2x'x''$ eigentlich darstellbar; es besteht daher eine Gleichung von der Form:

$$(25) \quad (\alpha t + \beta u)^2 - 2(\alpha' t + \beta' u)(\alpha'' t + \beta'' u) = \mu t^2 - 2\nu'' tu + \mu' u^2,$$

während die drei Zahlen

$$(26) \quad a = \alpha\beta' - \alpha'\beta, \quad b = \alpha'\beta'' - \alpha''\beta', \quad c = \alpha''\beta - \alpha\beta''$$

ohne gemeinsamen Theiler sind; auch können $a, 2b, c$ keinen solchen haben d. h. a und c nicht gleichzeitig gerade sein,

*) Im dritten Abschnitte dieses Werkes.

denn aus den Identitäten

$$a\alpha'' + b\alpha + c\alpha' = 0, \quad a\beta'' + b\beta + c\beta' = 0$$

würden in diesem Falle $b\alpha$ und $b\beta$ und, da in demselben b ungerade sein müsste, α und β sich als gerade Zahlen erweisen, wo dann, gegen die Voraussetzung, auch μ, μ' wegen (25) gerade sein müssten. Man nehme also etwa a als ungerade an. Da nun die Form (24) durch die Form f_1 eigentlich darstellbar ist, so ist die Determinante D durch die Reciproke von f_1, das ist aber die Form $x^2 - 2x'x''$, mittels der Zahlen

$$\alpha'\beta'' - \alpha''\beta', \quad \alpha''\beta - \alpha\beta'', \quad \alpha\beta' - \alpha'\beta$$

darstellbar, sodass die Gleichung besteht

$$D = b^2 - 2ac; \tag{27}$$

folglich ist $(a, -b, 2c)$ eine eigentlich-primitive Form mit der Determinante D. Aus (25) aber fliessen nachstehende Gleichungen:

für $t = \beta'$, $u = -\alpha'$:

$$a^2 = \mu\beta'^2 + 2\nu''\beta'\alpha' + \mu'\alpha'^2$$

für $t = \beta''$, $u = -\alpha''$:

$$c^2 = \mu\beta''^2 + 2\nu''\beta''\alpha'' + \mu'\alpha''^2$$

für $t = \beta$, $u = -\alpha$:

$$2ac = \mu\beta^2 + 2\nu''\beta\alpha + \mu'\alpha^2$$

für $t = \beta + \beta'$, $u = -\alpha - \alpha'$:

$$-ab = \mu\beta\beta' + \nu''(\alpha\beta' + \alpha'\beta) + \mu'\alpha\alpha'$$

für $t = \beta + \beta''$, $u = -\alpha - \alpha''$:

$$-bc = \mu\beta\beta'' + \nu''(\alpha\beta'' + \alpha''\beta) + \mu'\alpha\alpha''$$

für $t = \beta' + \beta''$, $u = -\alpha' - \alpha''$:

$$b^2 - ac = \mu\beta'\beta'' + \nu''(\alpha'\beta'' + \alpha''\beta') + \mu'\alpha'\alpha''$$

also

$$2b^2 = \mu(2\beta'\beta'' + \beta^2) + 2\nu''(\alpha'\beta'' + \alpha''\beta' + \alpha\beta) + \mu'(2\alpha'\alpha'' + \alpha^2).$$

Dieselben lassen unmittelbar erkennen, dass

$$\begin{cases}(ax^2 - 2bxy + 2cy^2)\cdot(ax'^2 - 2bx'y' + 2cy'^2) \\ \qquad = \mu X^2 + 2\nu'' XY + \mu' Y^2\end{cases} \tag{28}$$

ist, wenn man

$$X = \beta' x x' + \beta x y' + \beta x' y + 2\beta'' y y'$$
$$Y = \alpha' x x' + \alpha x y' + \alpha x' y + 2\alpha'' y y'$$

setzt, die Classe, welcher die Form (μ, ν'', μ') angehört, entsteht also durch Duplikation. In der That, wählt man, was möglich ist, x, y; x', y' so, dass die Form $(a, -b, 2c)$ eine gegen $2D$ prime Zahl M darstellt, so wird M^2 nach (28) durch (μ, ν'', μ') dargestellt, und, falls diese Darstellung keine eigentliche sein sollte, doch ein quadratischer Divisor von M^2 durch jene Form eigentlich dargestellt, was (s. analyt. Zahlenth. S. 258) die Behauptung begründet. Nun ist aber die Classe, welcher die Form (μ, ν'', μ') angehört, eine beliebige Classe des Hauptgeschlechtes; man erschliesst mithin auf diese Weise aus der Theorie der ternären quadratischen Formen einen der schönsten Sätze, die Gauss für binäre quadratische Formen festgestellt hat:

Jede Classe des Hauptgeschlechtes entsteht durch Duplikation.

Da auch jede Classe, welche durch Duplikation entsteht, umgekehrt zum Hauptgeschlechte gehört, so kommt dieser Satz überein mit der Gleichheit:

$$K(D) = Q(D). \tag{29}$$

Eine unmittelbare Folge dieser und der Gleichungen (6) und (7) ist die andere:

$$G(D) = \mathfrak{A}(D). \tag{30}$$

Bedient man sich nun des Gauss'schen Ausdrucks für die Anzahl der ambigen Classen, so ergiebt sich hieraus auch der Ausdruck für die Anzahl der Geschlechter und mit demselben der Satz: Die Anzahl der Geschlechter binärer Formen einer gegebenen Determinante ist halb so gross wie die Anzahl aller für letztere angebbaren Gesammtcharaktere. War also bereits gefunden, dass nur der einen Hälfte all' dieser Gesammtcharaktere Geschlechter entsprechen können, so ersieht man jetzt, dass auch wirklich zu jedem Gesammtcharakter dieser Hälfte ein Geschlecht binärer Formen vorhanden ist. Oder: die Beziehung (21) zwischen den Einzelcharakteren eines Geschlechts

ist für das Vorhandensein dieses Geschlechts nicht nur erforderlich, sondern auch ausreichend.

Auf Grund dieser letzteren Bedingungsgleichung, also unter Voraussetzung des Reciprocitätsgesetzes hat Dirichlet die Anzahl der Geschlechter ohne die allgemeine Bestimmung der Anzahl der ambigen Classen, wie sie Gauss gelehrt hat, auf analytischem Wege bestimmt*). Da hier das Reciprocitätsgesetz nach der Methode des zweiten Gauss'schen Beweises, jedoch unabhängig von jener allgemeinen Bestimmung der Anzahl der Ambigen begründet worden ist, würde nichts im Wege stehen, zur Bestimmung der Anzahl der Geschlechter jetzt den Dirichlet'schen Weg zu beschreiten, auf ihm also den zuletzt ausgesprochenen Satz unabhängig von Gauss und zugleich a posteriori vermittelst der Gleichung (30) den allgemeinen Ausdruck für die Anzahl der Ambigen wieder zu gewinnen.

b) Die ternären Formen.

6. Aber wir wenden uns nun wieder von den binären Formen zu den ternären zurück. Das für die ersteren erhaltene Resultat lässt sich verwenden zu dem Nachweise, dass die im zweiten Capitel definirten möglicherweise vorhandenen Geschlechter ternärer quadratischer Formen stets auch wirklich vorhanden sind.

Bezeichnet (Ω, Δ) eine gegebene Ordnung ternärer quadratischer Formen, so ist die Frage, ob es eine Form f dieser Ordnung giebt von der Art, dass, wenn $\mathfrak{F}$ ihre Reciproke bedeutet, die Symbole

$$\left(\frac{f}{\omega}\right), \left(\frac{f}{\omega'}\right), \cdots \left(\frac{\mathfrak{F}}{\delta}\right), \left(\frac{\mathfrak{F}}{\delta'}\right), \cdots,$$

in denen $\omega, \omega', \ldots$ die sämmtlichen verschiedenen Primfaktoren von Ω; $\delta, \delta', \ldots$ die sämmtlichen verschiedenen Primfaktoren von Δ bezeichnen, vorgeschriebene Werthe haben.

Sei nun M'' eine positive zu $2\Omega\Delta$ prime Zahl, für welche die Gleichungen

$$(31) \qquad \left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right), \left(\frac{M''}{\delta'}\right) = \left(\frac{\mathfrak{F}}{\delta'}\right), \cdots$$

*) S. Analytische Zahlentheorie, Abschnitt 9.

sowie die Congruenzbedingung

$$M'' \equiv \Omega \pmod{4}$$

erfüllt sind, wie es solche Zahlen stets giebt; mit $\mu, \mu', \ldots$ bezeichnen wir ihre verschiedenen Primfaktoren. Dann giebt es dem in voriger nr. Bewiesenen zufolge stets ein Geschlecht (ev. positiver) eigentlich-primitiver binärer Formen mit der Determinante

$$D = -\Omega M'' \equiv 3 \pmod{4},$$

deren Einzelcharaktere, wenn φ jede durch eine Form dieses Geschlechts darstellbare positive, zu $2D$ prime Zahl bedeutet, die folgenden Bedingungen:

$$(32) \qquad \begin{cases} \left(\frac{\varphi}{\omega}\right) = \left(\frac{f}{\omega}\right), \quad \left(\frac{\varphi}{\omega'}\right) = \left(\frac{f}{\omega'}\right), \cdots \\ \left(\frac{\varphi}{\mu}\right) = \left(\frac{-\varDelta}{\mu}\right), \left(\frac{\varphi}{\mu'}\right) = \left(\frac{-\varDelta}{\mu'}\right), \cdots \\ \text{und} \\ \qquad (-1)^{\frac{\varphi-1}{2}} = \left(\frac{\varphi}{\Omega M''}\right) \end{cases}$$

erfüllen; denn die letzte dieser Bedingungen lässt sich, da

$$-\Omega M'' \equiv 3 \pmod{4}$$

ist, auch so schreiben:

$$1 = (-1)^{\frac{\varphi-1}{2} \cdot \frac{\Omega M''+1}{2}} \cdot \left(\frac{\varphi}{\Omega M''}\right)$$

und erweist sich als identisch mit der Dirichlet'schen Bedingungsgleichung für die Existenz eines dem Gesammtcharakter (32) entsprechenden Geschlechtes binärer Formen mit der Determinante D. Als Repräsentanten irgend einer Classe dieses Geschlechts dürfen wir eine Form (m, n'', m') wählen, deren erster Coefficient positiv und prim ist gegen $2\Omega M''$. Da alsdann die Gleichungen stattfinden:

$$(33) \qquad \begin{cases} \left(\frac{m}{\omega}\right) = \left(\frac{f}{\omega}\right), \quad \left(\frac{m}{\omega'}\right) = \left(\frac{f}{\omega'}\right), \cdots \\ \left(\frac{m}{\mu}\right) = \left(\frac{-\varDelta}{\mu}\right), \left(\frac{m}{\mu'}\right) = \left(\frac{-\varDelta}{\mu'}\right), \cdots \\ \qquad (-1)^{\frac{m-1}{2}} = \left(\frac{m}{\Omega M''}\right), \end{cases}$$

so ist für jeden in M'' aufgehenden Primfaktor μ

$$\left(\frac{-\Delta m}{\mu}\right) = 1$$

also $-\Delta m$ quadratischer Rest von μ, und also auch von M'', mithin ist nach nr. 4 des dritten Capitels die Congruenzbedingung

$$(Ny - N'y')^2 + \Delta(my^2 + 2n''yy' + m'y'^2) \equiv 0 \pmod{M''}$$

erfüllbar und somit die Form (m, n'', m') als Bestandtheil in einer ternären Form $\begin{pmatrix} m, m', m'' \\ n, n', n'' \end{pmatrix}$ mit der Determinante $\Omega^2\Delta$ und mit der Reciproken $\begin{pmatrix} M, M', M'' \\ N, N', N'' \end{pmatrix}$ enthalten, während die Ordnung der ternären Form, da M'' und m positiv sind, die Ordnung $(+\Omega, \Delta)$ ist. Hiernach giebt es eine ternäre quadratische Form von der Ordnung (Ω, Δ), deren durch die Zahlen m und M'' gelieferten Einzelcharaktere nach (31) und (33) die vorgeschriebenen Werthe haben, und folglich gehört zu jedem der angebbaren Gesammtcharaktere wirklich ein Geschlecht ternärer quadratischer Formen der Ordnung (Ω, Δ).

7. Wir können die Betrachtung des Geschlechts ternärer Formen nicht verlassen, ohne einer Definition desselben Raum zu geben, die auf einer, von der bisherigen ganz verschiedenen Grundlage ruht. St. Smith hat zuerst den Beweis geführt*), dass, wenn eine ternäre quadratische Form f der Ordnung (Ω, Δ) durch eine Substitution mit dem Modulus Eins und mit rationalen Coefficienten, deren Generalnenner prim sei zu $2\Omega\Delta$, transformirt wird, die entstehende Form, wenn sie ganzzahlig ist, dem-

*) Man bemerke hierzu jedoch, was Hermite (J. f. Math. 52 S. 2) sagt: J'ai trouvé qu'elles jouissent de cette propriété arithmétique générale, que pour un système donné de valeurs des invariants les formes des diverses classes sont transformables les unes dans les autres par des substitutions linéaires au déterminant un, mais à coefficiens fractionnaires, c'est-à-dire, en adoptant la notion proposée par Mr. Eisenstein, que les diverses classes ne forment qu'un genre. Eisenstein ist wohl der Erste gewesen, welcher aus der rationalen Transformation der Formen den Gesichtspunkt zur Eintheilung der letzteren in Geschlechter entnommen hat (Monatsb. der Berl. Ak. 1852 S. 350).

selben Geschlechte angehört wie f, dass aber auch umgekehrt zwei Formen desselben Geschlechts durch solche Substitutionen in einander transformirt werden können.

Sei, um dies nachzuweisen,

$$(34)\qquad \begin{cases} x = \frac{\alpha_0{}^0}{n} y + \frac{\alpha_0{}'}{n} y' + \frac{\alpha_0{}''}{n} y'' \\ x' = \frac{\alpha_1{}^0}{n} y + \frac{\alpha_1{}'}{n} y' + \frac{\alpha_1{}''}{n} y'' \\ x'' = \frac{\alpha_2{}^0}{n} y + \frac{\alpha_2{}'}{n} y' + \frac{\alpha_2{}''}{n} y'' \end{cases}$$

eine Substitution vom Modulus 1, deren Coefficienten rational sind und den Generalnenner n haben. Die umgekehrte Substitution wird, bei Anwendung früherer Zeichen, die folgende sein:

$$(35)\qquad \begin{cases} y = \frac{A_0{}^0}{n^2} x + \frac{A_1{}^0}{n^2} x' + \frac{A_2{}^0}{n^2} x'' \\ y' = \frac{A_0{}'}{n^2} x + \frac{A_1{}'}{n^2} x' + \frac{A_2{}'}{n^2} x'' \\ y'' = \frac{A_0{}''}{n^2} x + \frac{A_1{}''}{n^2} x' + \frac{A_2{}''}{n^2} x''. \end{cases}$$

Geht nun durch die Substitution (34) die ternäre Form f in eine ganzzahlige Form f_1 über, so verwandelt sich bekanntlich durch die transponirte Substitution (35) die Adjungirte F von f in die ebenfalls ganzzahlige Adjungirte F_1 von f_1, durch die transponirte Substitution (34) aber umgekehrt F_1 in F. Aus dem ersten Grunde sind die Coefficienten von F_1 homogene lineare Funktionen der Coefficienten von F und quadratische Funktionen der Grössen $\frac{A_k^i}{n^2}$; heissen also Ω, Ω_1 resp. die grössten gemeinsamen Theiler aller Coefficienten von F und F_1, so muss nothwendig $\Omega_1 \cdot n^4$ durch Ω theilbar sein, und somit ist, falls n prim gegen $2\Omega\Delta$ angenommen wird, Ω_1 theilbar durch Ω. Umgekehrt sind die Coefficienten von F homogene lineare Funktionen derjenigen von F_1 und quadratisch in den Substitutionscoefficienten $\frac{\alpha_k^i}{n}$; daher muss $n^2 \cdot \Omega$ nothwendig durch Ω_1 theilbar sein. Nun sind, da die Substi-

tution (34) unimodular vorausgesetzt ist, die Determinanten der Formen f und f_1 einander gleich; f_1 ist eine primitive Form,

$$\Omega_1^2 \Delta_1 = \Omega^2 \Delta,$$

und folglich n auch prim gegen $2\Omega_1\Delta_1$, wenn es prim gegen $2\Omega\Delta$ vorausgesetzt wird; bei dieser Voraussetzung schliesst man daher aus dem Bewiesenen, dass Ω theilbar sein muss durch Ω_1. In Verbindung damit, dass es auch umgekehrt war, findet sich also die Gleichheit

$$\Omega_1 = \Omega \text{ und folglich auch } \Delta_1 = \Delta.$$

Die Formen f und f_1 gehören mithin zur selbigen Ordnung. Sie gehören aber auch demselben Geschlechte an. Denn, da vermöge der Substitution (34) die Gleichheit

$$f(x, x', x'') = f_1(y, y', y'')$$

besteht, wird für

$$y = nz, \quad y' = nz', \quad y'' = nz''$$

und ganzzahlige z, z', z''

$$f(x, x', x'') = n^2 \cdot f_1(z, z', z''),$$

der quadratische Charakter der Formen f und f_1 in Bezug auf alle Faktoren von $8\Omega\Delta$ also der gleiche sein. Und dasselbe gilt aus ähnlichen Gründen für die beiden reciproken Formen $\mathfrak{F}$ und $\mathfrak{F}_1$.

8. Somit ist der behauptete Satz in seinem ersten Theile bewiesen. Der Nachweis des anderen Theiles d. i. der Umkehrung des soeben Bewiesenen gründet sich auf folgenden, der Lehre von den binären Formen entnommenen

Hilfssatz: Sind φ_1, φ_2 zwei binäre quadratische Formen gleichen Geschlechts, so folgt aus der Auflösbarkeit der Gleichung:

$$\varphi_1(x, y) = M \tag{36}$$

stets auch die der Gleichung

$$\varphi_2(x, y) = Mz^2, \tag{37}$$

in welcher z als eine gegen die beliebig gegebene Zahl N prime ganze Zahl gedacht werden darf. Um dies zu zeigen, darf man offenbar φ_1, φ_2 durch jede ihnen äquivalente Form ersetzen. Da sie aber gleichem Geschlechte

angehören, giebt es in ihren Classen zwei Formen ψ_1, ψ_2 und im Hauptgeschlechte eine Form χ so beschaffen, dass

$$\psi_2 = \chi \cdot \psi_1$$

oder, weil jede Form des Hauptgeschlechtes durch Duplikation einer eigentlich-primitiven Form ψ entsteht,

$$\psi_2 = \psi^2 \cdot \psi_1$$

gesetzt werden kann. Ist nun die Gleichung (36) möglich, so lassen sich auch die Veränderlichen in ψ_1 so wählen, dass $\psi_1 = M$, und die Veränderlichen in der Form ψ so, dass ψ einen zu N primen Werth z erhält; mithin findet sich

$$\psi_2 = Mz^2,$$

also für geeignete Werthe von x, y auch die Gleichung (37).

Nun seien f_1, f_2 zwei ternäre, falls sie bestimmte Formen sind, positive Formen desselben Geschlechts, $\mathfrak{F}_1, \mathfrak{F}_2$ ihre Reciproken. Dann können, wenn m_1, m_2 zwei positive zu $2\Omega\Delta$ prime Zahlen bezeichnen, welche durch f_1 resp. f_2 eigentlich darstellbar sind und so gedacht werden können, dass

$$\Delta m_1 \equiv \Delta m_2 \equiv 1 \pmod{4}$$

ist, gleichzeitig mit ihnen durch $\mathfrak{F}_1, \mathfrak{F}_2$ zwei ebenfalls positive zu $2\Omega\Delta$ prime Zahlen M_1'', M_2'' eigentlich dargestellt werden. Seien

$$m_1 = f_1(\alpha_0^0, \alpha_1^0, \alpha_2^0), \quad M_1'' = \mathfrak{F}_1(\mathsf{A}_0'', \mathsf{A}_1'', \mathsf{A}_2'')$$

die gleichzeitigen Darstellungen von m_1 und M_1''; da für solche die Bedingung

$$\alpha_0^0 \mathsf{A}_0'' + \alpha_1^0 \mathsf{A}_1'' + \alpha_2^0 \mathsf{A}_2'' = 0$$

erfüllt sein muss, lassen sich drei andere Zahlen $\alpha_0', \alpha_1', \alpha_2'$ so angeben, dass

$$\mathsf{A}_0'' = \alpha_1^0\alpha_2' - \alpha_2^0\alpha_1', \quad \mathsf{A}_1'' = \alpha_2^0\alpha_0' - \alpha_0^0\alpha_2', \quad \mathsf{A}_2'' = \alpha_0^0\alpha_1' - \alpha_1^0\alpha_0'$$

ist. Die Darstellung von M_1'' ist alsdann der eigentlichen Darstellung einer binären Form φ_1 mit der Determinante $-\Omega M_1''$ durch die Form f_1 mittels der Formeln

$$\begin{aligned} x &= \alpha_0^0 y + \alpha_0' y' \\ x' &= \alpha_1^0 y + \alpha_1' y' \\ x'' &= \alpha_2^0 y + \alpha_2' y' \end{aligned}$$

zugeordnet; der erste Coefficient der Form φ_1 ist mithin m_1.

In gleicher Weise ist die Darstellung von M_2'' der eigentlichen Darstellung einer Form φ_2 mit der Determinante $-\Omega M_2''$ und dem ersten Coefficienten m_2 durch die Form f_2 zugeordnet. Die Formen φ_1, φ_2 sind eigentlich primitiv und, falls f_1, f_2 bestimmte Formen sind, positiv. Ferner gelten bezüglich jeden Primfaktors ω von Ω die Gleichungen

$$\left(\frac{\varphi_1}{\omega}\right) = \left(\frac{f_1}{\omega}\right), \quad \left(\frac{\varphi_2}{\omega}\right) = \left(\frac{f_2}{\omega}\right)$$

also, da f_1, f_2 gleichen Geschlechts sind, die Gleichung

$$\left(\frac{\varphi_1}{\omega}\right) = \left(\frac{\varphi_2}{\omega}\right).$$

Ist ferner μ ein in M_1'' und M_2'' gemeinsam enthaltener Primfaktor, so folgt aus den Gleichungen

$$\left(\frac{\varphi_1}{\mu}\right) = \left(\frac{-\Delta}{\mu}\right), \quad \left(\frac{\varphi_2}{\mu}\right) = \left(\frac{-\Delta}{\mu}\right)$$

die andere:

$$\left(\frac{\varphi_1}{\mu}\right) = \left(\frac{\varphi_2}{\mu}\right).$$

Man ersieht hieraus, dass die quadratischen Charaktere der beiden Formen φ_1, φ_2 mit Bezug auf die ihren Determinanten gemeinsamen Primfaktoren, ebenso auch — zugleich mit denen ihrer ersten Coefficienten — mit Bezug auf den Modulus 4 übereinstimmen, also mit einander verträglich sind. Es giebt deshalb gewisse arithmetische Reihen der Art, dass die bezüglichen quadratischen Charaktere der in ihnen enthaltenen Zahlen den Gesammtcharakteren der einen wie der anderen Form gleich sind, und unter diesen Zahlen befinden sich unendlich viel positive und negative Primzahlen, also auch eine nicht in $2\Omega\Delta$ enthaltene Primzahl p desselben Vorzeichens wie Ω, und für diese ist $\Delta p \equiv 1$ (mod. 4). Sie kann sowohl durch eine Form des Geschlechts von φ_1, als auch durch eine solche des Geschlechts von φ_2 dargestellt werden und daher giebt es nach dem Hilfssatze zwei zu $2\Omega\Delta$ prime Zahlen z_1, z_2 so beschaffen, dass pz_1^2 durch φ_1, pz_2^2 durch φ_2 selbst darstellbar sind; offenbar dürfen zudem letztere Darstellungen als eigentliche gedacht werden. Die Zahlen pz_1^2, pz_2^2 sind mithin auch durch die Formen f_1, f_2 resp. eigentlich darstellbar.

Man denke sich nun zwei ungerade Zahlen M_1, M_2, welche gleichzeitig mit jenen durch $\mathfrak{F}_1, \mathfrak{F}_2$ resp. eigentlich dargestellt werden. Da die Einheit

$$E = (-1)^{\frac{\Delta m+1}{2} \cdot \frac{\Omega M+1}{2}}$$

für je zwei gleichzeitig durch $f_1, \mathfrak{F}_1$ oder $f_2, \mathfrak{F}_2$ dargestellte ungerade Zahlen m, M einen gleichen Werth hat, die Zahlen pz_1^2, pz_2^2 aber den Congruenzen

$$\Delta pz_1^2 + 1 \equiv \Delta pz_2^2 + 1 \equiv 2 \pmod{4}$$

genügen, werden M_1, M_2 (mod. 4) congruent sein. Wendet man daher das obige Räsonnement statt auf die Formen f_1, f_2 jetzt auf $\mathfrak{F}_1, \mathfrak{F}_2$ an, so erkennt man einerseits die Existenz zweier eigentlich-primitiven binären Formen Φ_1, Φ_2, welche eine eigentliche Darstellung durch $\mathfrak{F}_1, \mathfrak{F}_2$ gestatten, denen diejenigen von pz_1^2, pz_2^2 durch f_1, f_2 resp. zugeordnet sind, sodass z. B.

$$\Phi_1(x, x') = \mathfrak{F}_1(\lambda_0^0 x + \lambda_0' x',\ \lambda_1^0 x + \lambda_1' x',\ \lambda_2^0 x + \lambda_2' x')$$
$$pz_1^2 = f_1(\lambda_1^0 \lambda_2' - \lambda_2^0 \lambda_1',\ \lambda_2^0 \lambda_0' - \lambda_0^0 \lambda_2',\ \lambda_0^0 \lambda_1' - \lambda_1^0 \lambda_0')$$

ist, andererseits die Existenz zweier durch Φ_1, Φ_2 resp. eigentlich darstellbarer Zahlen PZ_1^2, PZ_2^2, unter P eine Primzahl, unter Z_1, Z_2 ganze Zahlen verstanden, die alle prim sind gegen $2\Omega\Delta$.

Man hat also z. B. für passende Werthe von x, x'

$$PZ_1^2 = \mathfrak{F}_1(\lambda_0^0 x + \lambda_0' x',\ \lambda_1^0 x + \lambda_1' x',\ \lambda_2^0 x + \lambda_2' x')$$
$$pz_1^2 = f_1(\lambda_1^0 \lambda_2' - \lambda_2^0 \lambda_1',\ \lambda_2^0 \lambda_0' - \lambda_0^0 \lambda_2',\ \lambda_0^0 \lambda_1' - \lambda_1^0 \lambda_0')$$

d. i. zwei gleichzeitige eigentliche Darstellungen der Zahlen pz_1^2, PZ_1^2 durch f_1 und $\mathfrak{F}_1$; demnach giebt es eine mit f_1 äquivalente Form

$$g_1 = \begin{pmatrix} a_1, & a_1', & a_1'' \\ b_1, & b_1', & b_1'' \end{pmatrix},$$

deren erster Coefficient $a_1 = pz_1^2$, in deren Reciproken aber der dritte Coefficient $\mathfrak{A}_1'' = PZ_1^2$ ist. Ebenso giebt es eine mit f_2 äquivalente Form

$$g_2 = \begin{pmatrix} a_2, & a_2', & a_2'' \\ b_2, & b_2', & b_2'' \end{pmatrix},$$

deren erster Coefficient $a_2 = pz_2^2$, in deren Reciproken aber der dritte Coefficient $\mathfrak{A}_2'' = PZ_2^2$ ist. Den Gleichungen

$$a_1\mathfrak{A}_1''g_1 = \mathfrak{A}_1''(a_1x + b_1''x' + b_1'x'')^2 + \Omega(\mathfrak{A}_1''x' - \mathfrak{B}_1x'')^2 + a_1\Omega\Delta x''^2$$

$$a_2\mathfrak{A}_2''g_2 = \mathfrak{A}_2''(a_2x + b_2''x' + b_2'x'')^2 + \Omega(\mathfrak{A}_2''x' - \mathfrak{B}_2x'')^2 + a_2\Omega\Delta x''^2$$

zufolge geht dann die Form

$$\frac{1}{pP}(PX^2 + \Omega X'^2 + p\Omega\Delta X''^2)$$

mit rationalen Coefficienten durch die Substitution

$$\begin{aligned} X &= \frac{a_1}{z_1}x + \frac{b_1''}{z_1}x' + \frac{b_1'}{z_1}x'' \\ X' &= \frac{\mathfrak{A}_1''}{z_1Z_1}x' - \frac{\mathfrak{B}_1}{z_1Z_1}x'' \\ X'' &= \frac{1}{Z_1}x'' \end{aligned}$$

mit dem Modulus pP in die Form g_1, durch die Substitution

$$\begin{aligned} X &= \frac{a_2}{z_2}x + \frac{b_2''}{z_2}x' + \frac{b_2'}{z_2}x'' \\ X' &= \frac{\mathfrak{A}_2''}{z_2Z_2}x' - \frac{\mathfrak{B}_2}{z_2Z_2}x'' \\ X'' &= \frac{1}{Z_2}x'' \end{aligned}$$

mit demselben Modulus in die Form g_2 über, und somit verwandelt sich durch eine unimodulare Substitution mit rationalen Coefficienten, deren Generalnenner, ebenso wie z_1, z_2, Z_1, Z_2 nur prim gegen $2\Omega\Delta$ sein kann, g_1 in g_2; Gleiches gilt dann offenbar von den mit g_1, g_2 resp. äquivalenten Formen f_1, f_2 w. z. b. w.

Sechstes Capitel.

Positive Formen. Die Form $x^2 + x'^2 + x''^2$.

1. Von nun an beschränken wir uns zunächst ganz auf positive Formen der Ordnung (Ω, Δ), für welche demnach

$\Omega > 0$ ist. Vor allem ist eine Betrachtung anzustellen, welche Eisenstein zur Einführung eines neuen sehr wichtigen Begriffes veranlasst hat.

Wendet man auf eine positive ternäre Form sämmtliche Substitutionen an, deren Modulus 1 ist, so erhält man alle zu ihr äquivalenten Formen, jede von ihnen gleich oft, denn unter jenen Substitutionen befinden sich auch diejenigen Substitutionen in endlicher Anzahl θ, welche die Form in sich selbst verwandeln und genau so oft, wie in sich selbst, verwandelt sich (nach nr. 5 des ersten Capitels) die Form in jede ihr äquivalente. Nun fand man die sämmtlichen Transformationen einer Form f in sich selbst mittels der ganzzahligen Auflösungen gewisser Gleichungen von der Form

$$t^2 + F(u, u', u'') = \Theta,$$

wo F die Adjungirte von f und Θ eine von der Determinante von f abhängige Zahl bedeutet. Demnach wird ihre Anzahl θ mit der Form f selbst veränderlich sein, ganz abweichend von den binären Formen, bei welchen die Transformationen in sich selbst mittels der Auflösungen der Pell'schen Gleichung bestimmt werden, ihre Anzahl also nur abhängig ist von der Determinante und deshalb für alle Formen gleicher Determinante gleich gross. Da aber das System aller unimodularen Substitutionen für jede Form f dasselbe ist, giebt es offenbar um so mehr mit f äquivalente Formen, die Classe, welcher f angehört, wird um so dichter an Formen sein, je kleiner θ oder je grösser $\frac{1}{\theta}$ ist, oder die Anzahl Formen einer Classe ist proportional mit diesem Bruche, welcher deshalb als *das Maass* (oder die Dichtigkeit, nach Smith: weight) dieser Classe, sowie *jeder zu ihr gehörigen Form* benannt werden darf.

Nennt man τ die Anzahl der Transformationen einer binären Form in sich selbst, so würde in gleicher Weise $\frac{1}{\tau}$ das Maass dieser Form oder ihrer Classe sein, ein Werth, der nach dem Gesagten für jede binäre Form derselben Determinante derselbe, für positive (primitive) Formen im Allgemeinen $\frac{1}{2}$ ist.

Da jeder Transformation einer Form f in sich selbst eine solche ihrer Reciproken in sich selbst entspricht und umgekehrt, so ist das Maass für zwei zu einander reciproke Formen stets dasselbe.

Hat man mehrere Classen C_i, z. B. diejenigen eines Geschlechts oder einer Ordnung, so kann man die Summe ihrer Maasse, $\sum \frac{1}{\theta_i}$, als das Maass des Geschlechts resp. der Ordnung bezeichnen.

Der Begriff des Maasses einer Form überträgt sich auch auf jede durch sie dargestellte Zahl oder auf die entsprechende Darstellung selbst: Das Maass der Darstellung einer Zahl ist das Maass der Form, durch die sie geschieht. Dagegen nennt man Maass der Darstellung einer binären Form durch eine ternäre das Produkt aus dem Maasse der ersteren in das Maass der letzteren: $\frac{1}{\tau\theta}$; und wieder wird Maass eines Systems von Darstellungen, sei es von Zahlen, sei es von binären Formen, die Summe der Maasse aller jener resp. aller dieser sein.

Nach Einführung dieser wichtigen Eisenstein'schen Begriffe stellt sich nun von selbst die Aufgabe dar, das Maass eines gegebenen Geschlechts der Ordnung (Ω, Δ) oder dieser Ordnung selbst zu bestimmen, und wird im nächsten Capitel gelöst werden. An dieser Stelle soll vorläufig nur ein dahin zielender Satz hergeleitet werden, der sich aus den bisherigen Untersuchungen leicht erschliessen lässt.

2. Sei ein Geschlecht positiver Formen der Ordnung (Ω, Δ) gegeben dadurch, dass man den ihm entsprechenden Symbolen

$$\left(\frac{f}{\omega}\right), \left(\frac{f}{\omega'}\right), \cdots \left(\frac{\mathfrak{F}}{\delta}\right), \left(\frac{\mathfrak{F}}{\delta'}\right), \cdots$$

bestimmte Werthe beilegt. Versteht man unter M'' eine positive und zu $2\Omega\Delta$ prime Zahl, welche die Bedingungen

$$(1) \qquad \left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right), \left(\frac{M''}{\delta'}\right) = \left(\frac{\mathfrak{F}}{\delta'}\right), \cdots$$

und $M'' \equiv \Omega \pmod{4}$ erfüllt, so giebt es, wie im vorigen

Capitel gezeigt worden ist, ein bestimmtes Geschlecht (positiver) eigentlich-primitiver binärer Formen mit der Determinante $D = -\Omega M''$, dessen Classenrepräsentanten φ so gewählt werden können, dass die für die Darstellbarkeit durch eine Form der Ordnung (Ω, Δ) erforderliche Bedingung, nämlich die Congruenz

(2) $$(Ny - N'y')^2 + \Delta \cdot \varphi \equiv 0 \pmod{M''}$$

erfüllbar ist. Seien

(3) $$\varphi_1, \varphi_2, \dots \varphi_g$$

diese Repräsentanten der verschiedenen Classen des genannten Geschlechts. Um alle ihre eigentlichen Darstellungen durch die Ordnung (Ω, Δ) zu finden, muss man verfahren, wie es in nr. 6 des dritten Capitels auseinandergesetzt worden ist. Man bilde also zunächst für die Form φ_1 die dort mit (34) bezeichneten Formen. Man darf sich nun aber auf diejenigen Formen

(4) $$f_1, f_2, f_3, \dots$$

des dortigen Systems (32) beschränken, welche dem Geschlechte ternärer Formen, das man betrachtet, angehören; denn jede der Formen $f^{(i)}$ kann nur einer Form dieses Geschlechts äquivalent sein, da sie die Bedingungen

$$\left(\frac{f^{(i)}}{\omega}\right) = \left(\frac{\varphi_1}{\omega}\right) = \left(\frac{f}{\omega}\right), \dots$$

und ihre Reciproke $\mathfrak{F}^{(i)}$ zugleich die Bedingungen

$$\left(\frac{\mathfrak{F}^{(i)}}{\delta}\right) = \left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right), \dots$$

erfüllt. Ist wieder μ die Anzahl der verschiedenen Primfaktoren, aus denen M'' besteht, also 2^μ die Anzahl der Wurzeln der Congruenz (2), so ist die Anzahl der Formen $f^{(i)}$ ebenso gross. Angenommen nun, $f^{(i)}$ sei äquivalent mit f_1, so giebt es zunächst so viel von einander verschiedene eigentliche Darstellungen von φ_1 durch f_1, als es Transformationen von f_1 in $f^{(i)}$ oder auch in sich selbst giebt, deren Anzahl θ_1 heisse; das Maass jeder einzelnen dieser Darstellungen ist $\frac{1}{\tau\theta_1}$ und folglich das Maass ihrer Gesammtheit gleich $\frac{1}{\tau}\cdot$ Um alle ver-

schiedenen Darstellungen von φ_1 durch die Formen (4) zu erhalten, muss man diese Betrachtung für jede der Formen $f^{(i)}$ anstellen und findet dann offenbar $2^\mu \cdot \frac{1}{\tau}$ für das Maass sämmtlicher Darstellungen von φ_1 durch die Formen (4) des gegebenen Geschlechts; und wenn dieselbe Betrachtung für jede der Formen (3) wiederholt wird, ergiebt sich das Resultat:

Das Maass sämmtlicher eigentlichen Darstellungen der Classenrepräsentanten des gedachten Geschlechts binärer Formen durch das Formensystem des gegebenen ternären Geschlechts ist

$$(5) \qquad 2^\mu \cdot \frac{g}{\tau} \cdot$$

3. Man bezeichne mit

$$(6) \qquad \mathfrak{F}_1, \mathfrak{F}_2, \mathfrak{F}_3, \ldots$$

die Reciproken zu den Formen (4) des gegebenen Geschlechts. Jeder eigentlichen Darstellung einer der Formen (3) durch eine der Formen (4) ist bekanntlich eine eigentliche Darstellung von M'' durch die entsprechende Reciproke aus der Reihe (6) zugeordnet. — Ist umgekehrt M'' durch eine der letzteren Formen, etwa durch $\mathfrak{F}_1$ eigentlich darstellbar, so ist diese Darstellung der eigentlichen Darstellung einer binären Form φ mit der Determinante $-\Omega M''$ durch die Form f_1 zugeordnet; diese Form ist primitiv (nach nr. 3 des dritten Capitels) und zwar eigentlich, da die Determinante

$$\equiv 3 \pmod{4}$$

ist; und weil sie durch f_1 eigentlich darstellbar ist, muss die Congruenz (2) auflösbar, also die Gleichungen

$$\left(\frac{\varphi}{\mu}\right) = \left(\frac{-\Delta}{\mu}\right), \; \left(\frac{\varphi}{\mu'}\right) = \left(\frac{-\Delta}{\mu'}\right), \ldots$$

ebenso wie auch diese anderen:

$$\left(\frac{\varphi}{\omega}\right) = \left(\frac{f}{\omega}\right), \; \left(\frac{\varphi}{\omega'}\right) = \left(\frac{f}{\omega'}\right), \ldots$$

und endlich, da für das Geschlecht von φ die Dirichlet'sche Bedingungsgleichung statthaben muss, auch die folgende:

$$(-1)^{\frac{\varphi-1}{2}} = \left(\frac{\varphi}{\Omega M''}\right)$$

erfüllt sein, d. h. φ muss dem in voriger nr. bezeichneten Geschlechte binärer Formen angehörig und deshalb mit einer der Formen (3), etwa mit φ_1, äquivalent sein. Demnach ist dann die Darstellung von M'' auch einer eigentlichen Darstellung dieser letzteren Form durch f_1 zugeordnet, und zwar nicht nur einer, sondern (nach nr. 1, 4) des dritten Capitels) genau τ solchen Darstellungen. Das Maass der Darstellung von M'' durch $\mathfrak{F}_1$ ist aber $\frac{1}{\theta_1}$, das jeder einzelnen Darstellung von φ_1 durch die entsprechende Form f_1 ist $\frac{1}{\tau\theta_1}$, also das Maass sämmtlicher Darstellungen von φ_1 durch f_1, denen diejenige von M'' zugeordnet ist, gleich $\frac{1}{\theta_1}$. Denkt man folglich alle eigentlichen Darstellungen von M'' durch die Formen (6), so ist die Summe ihrer Maasse gleich der Summe der Maasse aller eigentlichen Darstellungen der Formen (3) durch die Formen (4), denen solche Darstellungen von M'' zugeordnet sind, d. h. aber nach der anfänglich gemachten Bemerkung sämmtlicher eigentlichen Darstellungen der Formen (3) durch die Formen (4) überhaupt, also gleich $2^\mu \cdot \frac{g}{\tau}$. Oder wir erhalten den Satz:

Ist M'' eine positive zu $2\Omega\Delta$ prime und mit Ω (mod. 4) congruente Zahl, welche die Bedingungen (1) erfüllt, und μ die Anzahl der verschiedenen Primfaktoren, aus denen sie besteht, so ist das Maass ihrer eigentlichen Darstellungen durch die Formen (6), welche den Repräsentanten (4) eines gegebenen Geschlechts ternärer Formen der Ordnung (Ω, Δ) reciprok sind, gleich 2^μ mal dem Maasse $\frac{g}{\tau}$ eines (durch die Gleichungen (32) vorigen Capitels) bestimmten Geschlechts positiver eigentlich-primitiver binärer Formen mit der Determinante $-\Omega M''$.

Da jedes Geschlecht solcher Formen gleichviel Classen enthält, darf hierbei unter g die Anzahl Classen ihres Hauptgeschlechts verstanden werden.

Die Form $x^2 + x'^2 + x''^2$.

4. Von den letztgefundenen allgemeinen Ergebnissen machen wir jetzt im Besonderen die Anwendung auf die ternären Formen der Ordnung (1, 1). Vorweg sei bemerkt, was erst an späterer Stelle bewiesen werden wird, dass alle diese Formen nur eine einzige Classe bilden, als deren Repräsentant die einfachste Form derselben, die Form

$$(7) \qquad f = x^2 + x'^2 + x''^2$$

genommen werden darf. Dieser Form ist es eigenthümlich, dass ihre Reciproke mit ihr identisch ist:

$$(8) \qquad \mathfrak{F} = x^2 + x'^2 + x''^2.$$

Da nur eine Classe vorhanden ist, giebt es auch nur ein einziges Geschlecht, das Hauptgeschlecht, welches gleichfalls durch die Form (7) repräsentirt wird. Auf diese einzige Form reducirt sich also das mit (4) bezeichnete System von Formen, sowie das mit (6) bezeichnete auf die einzige Form (8). Die im Vorigen mit M'' bezeichnete positive Zahl, die wir grösser als 1 denken, hat man hier nur der einzigen Bedingung zu unterwerfen, dass $M'' \equiv 1 \pmod{4}$ sei. Dem Schlusssatze der vor. nr. gemäss ist alsdann das Maass aller eigentlichen Darstellungen von M'' durch die Form $x^2 + x'^2 + x''^2$ gleich $2^\mu \cdot \frac{g}{\tau}$, wenn g die Anzahl Classen des Hauptgeschlechts binärer Formen mit der Determinante $-M''$ bezeichnet. Wegen $M'' > 1$ ist $\tau = 2$; ferner ist das Maass jeder eigentlichen Darstellung einer Zahl durch die Form $\mathfrak{F}$ gleich $\frac{1}{\theta}$, wenn θ die Anzahl der Transformationen von $\mathfrak{F}$ in sich selbst, also (nach nr. 3 des vierten Capitels) die Zahl 24 bezeichnet. Ist demnach A die Anzahl der eigentlichen Darstellungen von M'' durch $\mathfrak{F}$, so ist

$$(9) \qquad \frac{A}{24} = 2^\mu \cdot \frac{g}{2} \quad \text{oder } A = 3 \cdot 2^{\mu+2} \cdot g.$$

Auf solche Weise geht der Gauss'sche Satz*) hervor: Die Anzahl der eigentlichen Darstellungen einer

*) S. Disquis. Arithm. art. 291.

positiven Zahl M'' von der Form $4n+1$ als Summe dreier Quadrate ist $3\cdot 2^{\mu+2}\cdot g$, wenn μ die Anzahl der verschiedenen Primfaktoren bezeichnet, aus denen M'' besteht, und g die Anzahl der Classen im Hauptgeschlechte binärer eigentlich-primitiver quadratischer Formen von der Determinante $-M''$.

Für Zahlen M'' von der Form $8n+3$ besteht ein ähnlicher Satz: Die Anzahl der eigentlichen Darstellungen einer solchen Zahl als Summe dreier Quadrate ist $2^{\mu+2}\cdot g$. Doch kann dieser Satz, obwohl er auf ganz analogen Betrachtungen beruht, als für den Beweis des ersteren verwendet worden sind, aus unseren Entwickelungen nicht ohne weiteres abgeleitet werden, weil es dazu auch der Betrachtung uneigentlich-primitiver Formen bedürfen würde, die wir vermieden haben.

Die Zahlen von der Form $8n+7$ kommen nicht in Betracht, da solche durch die Form $x^2+x'^2+x''^2$ nicht darstellbar sind. In der That besteht für diese Form (s. (41) des zweiten Capitels) die Gleichung

$$E=-1$$

und folglich sind nur solche ungerade Zahlen durch die Form darstellbar, welche $\equiv 1, 3, 5$, nicht aber solche, welche $\equiv 7$ (mod. 8) sind. Dies leuchtet auch ohne weiteres ein; denn da $x^2+x'^2+x''^2$ nur dann von der Form $4n+3$ wird, wenn x, x', x'' ungerade sind, in diesem Falle aber von der Form $8n+3$ ist, kann eine Zahl von der Form $8n+7$ nicht Summe dreier Quadratzahlen sein.

In gleicher Weise überzeugt man sich, dass nur solche gerade Zahlen als Summe dreier Quadrate eigentlich darstellbar sind, welche die Form $4n+2$ haben.

Von den Darstellungen einer ungeraden Zahl als Summe dreier Quadrate sind ihre Zerlegungen in eine solche Summe zu unterscheiden, indem man bei den letzteren nur auf die Werthe der drei Quadrate, nicht aber auf ihre verschiedene Folge noch auf die Vorzeichen ihrer Grundzahlen Acht nimmt. Dann wird eine Zerlegung in drei von Null und von einander

verschiedene Quadrate offenbar je $1 \cdot 2 \cdot 3 \cdot 2^3 = 48$, eine Zerlegung, bei welcher ein Quadrat Null, die anderen also verschieden sind, je $1 \cdot 2 \cdot 3 \cdot 2^2 = 24$, oder bei welcher alle drei Quadrate von Null verschieden aber zwei gleich sind, je

$$3 \cdot 2^3 = 24$$

verschiedenen eigentlichen Darstellungen entsprechen. Finden sich demnach unter allen Z Zerlegungen in drei Quadrate resp. z und ζ solche von den beiden letzten Arten, so ist

$$\begin{aligned} A &= 48(Z - z - \zeta) + 24(z + \zeta) \\ &= 48Z - 24(z + \zeta).^{*)} \end{aligned}$$

Eine eigentliche Zerlegung $M'' = x^2 + x'^2$ ist aber nur dann möglich, wenn -1 quadratischer Rest von M'' ist, und dann giebt es deren $\frac{1}{8} \cdot 2^{\mu+2} = 2^{\mu-1}$; ebenso ist eine eigentliche Zerlegung $M'' = x^2 + 2x'^2$ nur möglich, wenn -2 quadratischer Rest von M'' ist, und dann giebt es deren

$$\frac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}.$$

Bezeichnet demnach $\varkappa$, jenachdem

$$M'' \equiv 1 \pmod{4} \quad \text{oder} \quad M'' \equiv 3 \pmod{8}$$

ist, $3g$ oder g, so kann man sagen:

es ist

$$(9a) \quad \begin{cases} Z = 2^{\mu-2} \cdot \frac{\varkappa}{3}, \\ \text{wenn } -1 \text{ und } -2 \text{ Nichtreste von } M''; \\ Z = 2^{\mu-2} \cdot \left(\frac{\varkappa}{3} + 1\right), \\ \text{wenn nur eine dieser Zahlen quadratischer Rest;} \\ Z = 2^{\mu-2} \cdot \left(\frac{\varkappa}{3} + 2\right), \\ \text{wenn sie beide quadratische Reste von } M'' \text{ sind.} \end{cases}$$

Ist insbesondere $M'' = 8n + 3$, so wird die erste oder zweite dieser Formeln gelten, jenachdem -2 quadratischer

---

*) Der Fall $M'' = 3$ ist auszunehmen, denn in ihm ist nur eine Zerlegung: $3 = 1^2 + 1^2 + 1^2$ vorhanden, bei welcher alle drei Quadrate gleich sind.

Nichtrest oder Rest von M'' ist, und da in diesem Falle $\varkappa = g$, so zeigen diese Formeln, was die Theorie der binären Formen bestätigt, dass die Anzahl der Classen im Hauptgeschlechte binärer Formen mit einer Determinante $-M'' \equiv 5 \pmod{8}$ ein Vielfaches von 3 ist.

Hier ist der Ort, mit Dirichlet (s. den Schluss seiner recherches sur l'application de l'analyse infinitésimale à la théorie des nombres, Crelle's Journal 21 S. 155) darauf hinzuweisen, wie man durch eine Combination seiner Formeln für die Classenanzahl mit den Gauss'schen Sätzen über die Anzahl der Darstellungen einer Zahl als Summe dreier Quadrate für diese letztere Anzahl sehr einfache Formeln gewinnen kann, die von jeder Beziehung auf binäre Formen befreit sind.

In der That, wenn man sich der Kürze wegen auf den Fall $M'' \equiv 1 \pmod{4}$ beschränkt, so kann man u. A. für die Anzahl $H(-M'')$ der Classen eigentlich-primitiver binärer Formen mit der Determinante $-M''$ folgende Formeln aufstellen:

$$1) \qquad H(-M'') = \frac{\Sigma\beta - \Sigma\alpha}{4M''}$$

$$2) \qquad H(-M'') = \frac{1}{2}(\mathfrak{A} - \mathfrak{B}),$$

in denen α, β alle zu $4M''$ primen Zahlen $< 4M''$ bedeuten, für welche resp.

$$(-1)^{\frac{\alpha-1}{2}} \cdot \left(\frac{\alpha}{M''}\right) = +1, \quad (-1)^{\frac{\beta-1}{2}} \cdot \left(\frac{\beta}{M''}\right) = -1$$

ist, während $\mathfrak{A}, \mathfrak{B}$ die Anzahl dieser Zahlen α, β sind, welche $2M''$ nicht übersteigen;

$$3) \qquad H(-M'') = 2(A - B),$$

wo A, B die Anzahl aller gegen M'' primen Zahlen a, b bezeichnen, welche $< \frac{M''}{4}$ sind und resp. die Gleichungen

$$\left(\frac{a}{M''}\right) = 1, \quad \left(\frac{b}{M''}\right) = -1$$

erfüllen, einfacher:

$$H(-M'') = 2 \cdot \sum_{1}^{\left[\frac{M''}{4}\right]} \left(\frac{s}{M''}\right),$$

falls man dem Symbole $\left(\frac{s}{M''}\right)$, so oft s und M'' einen gemeinsamen Theiler haben, den Werth Null beilegt. — Da nun

$$g=\frac{1}{2^\mu}\cdot H(-M'')$$

ist, findet man aus dem Gauss'schen Satze entsprechend folgende drei Formeln für die Anzahl A der eigentlichen Darstellungen von M'' als Summe von drei Quadraten:

$$(10)\qquad \begin{cases} 1)\ A=3\cdot\frac{\Sigma\beta-\Sigma\alpha}{M''} \\ 2)\ A=6(\mathfrak{A}-\mathfrak{B}) \\ 3)\ A=24\,.\sum_1^{\left[\frac{M''}{4}\right]}\left(\frac{s}{M''}\right), \end{cases}$$

von denen wohl die letzte die einfachste zu nennen ist.

Wenn $M''\equiv 3 \pmod{8}$ ist, so findet man ähnlich

$$(10a)\qquad A=8\cdot\sum_1^{\left[\frac{M''}{2}\right]}\left(\frac{s}{M''}\right).$$

5. Für die ausgezeichnete ternäre Form

$$f=x^2+x'^2+x''^2,$$

die wir soeben betrachtet, waren bereits vor Gauss die hauptsächlichsten Sätze seiner allgemeinen Darstellungstheorie von Legendre hergeleitet worden*), doch stellen sie sich bei ihm unter anderer Form dar, weil er sich einer den Mathematikern vor Gauss eigenthümlichen Ausdrucksweise bedient. So nennt er jede eigentliche Darstellung einer Zahl als Summe dreier Quadrate eine trinäre Form dieser Zahl, jede (positive) binäre quadratische Form der Determinante $-D$ heisst ein Theiler von t^2+Du^2, und, wenn sie einer eigentlichen Darstellung durch die Form $f=x^2+x'^2+x''^2$ fähig ist, ein trinärer Theiler dieses Ausdrucks. Hierbei gelten äquivalente binäre Formen nur als ein einziger Theiler desselben. Von den Methoden zwar, welche Legendre angewendet, seine Resultate zu erreichen, und welche durchweg elementarer Art

*) Legendre, théorie des Nombres.

sind, können wir hier keine Darstellung geben, aber es scheint zur Orientirung über die ältere zahlentheoretische Literatur nicht unwichtig, in Kürze das Verhältniss zu kennzeichnen, in welchem seine Betrachtungen zu der hier dargestellten Gaussschen Theorie stehen.

Vorweg ist zu bemerken, dass Legendre als verschiedene trinäre Formen einer Zahl oder einer binären Form φ nur die verschiedenen Zerlegungen derselben in die Summe dreier Quadrate zählt, daher die $\tau = 2$ Darstellungen von φ:

(11) $x = \alpha y + \beta y',\ x' = \alpha' y + \beta' y',\ x'' = \alpha'' y + \beta'' y'$

und

(11a) $x = -\alpha y - \beta y',\ x' = -\alpha' y - \beta' y',\ x'' = -\alpha'' y - \beta'' y',$

denen ein- und dieselbe Darstellung ihrer Determinante entspricht, nur eine einzige trinäre Form des Theilers φ geben. Dies vorausgeschickt, folgt zunächst aus nr. 1, 1) und 2) des dritten Capitels, wenn man daselbst die Form f und ihre Reciproke $\mathfrak{F}$ mit $x^2 + x'^2 + x''^2$ identificirt: Jedem trinären Theiler von $t^2 + M''u^2$ ist eine trinäre Form von M'' zugeordnet (Legendre nr. 269) und umgekehrt (L. nr. 272); auch kann (L. nr. 274) jede trinäre Form von M'' nur einem einzigen trinären Theiler von $t^2 + M''u^2$ zugeordnet sein (nach Capitel 3 nr. 1, 5)).

Ist aber eine Form (p, q, r) eigentlich durch f darstellbar mittels der Formeln (11) und $\mathsf{A}, \mathsf{A}', \mathsf{A}''$ die zugeordnete Darstellung von M'', so wird die entgegengesetzte Form $(p, -q, r)$ durch f dargestellt mittels der Formeln

$$x = \alpha y - \beta y', \quad x' = \alpha' y - \beta' y', \quad x'' = \alpha'' y - \beta'' y'$$

und die zugeordnete Darstellung von M'' ist

$$-\mathsf{A},\ -\mathsf{A}',\ -\mathsf{A}''.$$

Wenn nun die Form (p, q, r) einer ambigen Classe angehört, also äquivalent ist mit $(p, -q, r)$, so ist die letztere Darstellung (nach Cap. 3, nr. 1, 3)) auch einer Darstellung von (p, q, r) zugeordnet, welche von der Darstellung (11) oder (11a) verschieden sein muss. Die genannten beiden Darstellungen von M'' geben jedoch nur eine trinäre Form von M'':

$$M'' = \mathsf{A}^2 + \mathsf{A}'^2 + \mathsf{A}''^2.$$

Man findet also: Während im Allgemeinen jeder trinären Form von M'' nur eine einzige trinäre Form des zugeordneten Theilers von $t^2 + M''u^2$ entspricht, entsprechen ihr zwei solche Formen, so oft der Theiler ambige (nach Legendre's Ausdrucksweise: bifide) ist (L. nr. 275—278).

Wenn $\varphi = (p, q, r)$ eine Form der Determinante $-M''$, wenn ferner p, M'' relative Primzahlen und $-p$ quadratischer Rest ist von M'', P aber irgend eine durch (p, q, r) darstellbare zu M'' prime Zahl, so ist auch $-P$ quadratischer Rest von M'', also M'' durch eine Form ψ mit der Determinante $-P$ darstellbar. Dies folgt sogleich, wenn man

$$P = p\alpha^2 + 2q\alpha\beta + r\beta^2$$

annimmt, aus der Gleichung

$$p \cdot P = (p\alpha + q\beta)^2 + M''\beta^2.$$

Legendre nennt alsdann die Form φ einen reciproken Theiler von $t^2 + M''u^2$. Die Congruenz nun, deren Auflösbarkeit die nothwendige Bedingung für die eigentliche Darstellbarkeit einer Form φ durch die Form

$$f = x^2 + x'^2 + x''^2$$

ist, lautet folgendermassen:

$$(12) \qquad (Ny - N'y')^2 + \varphi \equiv 0 \pmod{M''};$$

für diese besondere Form f ist sie nach nr. 5 und 6 des dritten Capitels zugleich die ausreichende Bedingung der Darstellbarkeit, denn das Formensystem (32) daselbst reducirt sich im gegenwärtigen Falle auf die einzige Form f. Aus der Congruenz folgt aber für jede durch φ darstellbare Zahl P, dass $-P$ quadratischer Rest von M'' ist; und umgekehrt wird sie auflösbar (nach nr. 4 daselbst), wenn dies für irgend eine durch φ darstellbare, gegen M'' prime Zahl, z. B. für ihren ersten Coefficienten p erfüllt wird. Hieraus ergiebt sich offenbar: Jeder trinäre Theiler von $t^2 + M''u^2$ ist ein reciproker Theiler dieses Ausdrucks, und umgekehrt (L. nr. 302 und 304). Für den Fall $M'' \equiv 1 \pmod{4}$ wären hiernach die (nicht äquivalenten) reciproken Theiler jenes Aus-

drucks mit den durch $\varphi_1, \varphi_2, \ldots \varphi_g$ bezeichneten Formen in nr. 2 identisch.

Das Vorhandensein solcher Theiler — welches in dem angegebenen Falle sich aus dem im vorigen Capitel gegebenen Nachweise ergiebt, dass ein Geschlecht binärer Formen φ existirt, für welches die Congruenz (12) auflösbar ist — wird von Legendre in den nr. 293—301 allgemeiner untersucht. Aus den mitgetheilten Resultaten erschliesst er dann neben anderen ähnlichen Sätzen den Satz: dass jede ungerade Zahl, welche nicht die Form $8n+7$ hat, als Summe dreier Quadratzahlen darstellbar ist (L. nr. 317 sqq.).

6. Bewiesen haben wir diesen Satz bisher erst für die Zahlen von der Form $4n+1$, für diejenigen der Form $8n+3$ noch nicht; derselbe Satz gilt aber auch noch für die geraden Zahlen von der Form $4n+2$, so dass man aussagen darf:

Jede Zahl, welche keine der Formen $4n$ oder $8n+7$ hat, kann (eigentlich) in der Form

$$x^2 + x'^2 + x''^2$$

d. i. als Summe dreier Quadratzahlen (ohne gemeinsamen Theiler) dargestellt werden. Da dieser Satz zugleich den Ausgangspunkt für eine ganze Reihe weiterer, sehr interessanter Entwickelungen bildet, ist es nöthig, ihn in seiner ganzen Allgemeinheit zu beweisen; und wenn man dabei von der Anzahl der Darstellungen ab und nur auf die Möglichkeit der Darstellung sieht, lässt sich dieser Beweis, wie Dirichlet gezeigt hat*), ohne die allgemeine Gauss'sche Theorie mittels verhältnissmässig sehr einfacher Betrachtungen folgendermassen erbringen.

Es ist bereits bemerkt, dass alle ternären Formen der Ordnung (1, 1) oder, was dasselbe sagt, alle positiven ternären Formen mit der Determinante 1 nur eine Classe bilden, also sämmtlich der Form $x^2 + x'^2 + x''^2$ äquivalent sind. Giebt es mithin eine positive Form mit dieser Determinante, durch welche die gegebene positive Zahl a eigentlich darstellbar

---

*) Dirichlet, über die Zerlegbarkeit der Zahlen in drei Quadrate, Journ. f. Math. 40 S. 228, oder Journ. des Math. v. Liouville, 2. série, t. 4.

oder, noch bestimmter, eine solche Form, deren erster Coefficient gleich a ist, so ist a auch eigentlich darstellbar als Summe dreier Quadratzahlen. Demnach ist nur erforderlich zu zeigen, dass eine Form $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ vorhanden ist, welche folgende Bedingungen erfüllt:

erstens:

$$(13) \qquad aa'a'' + 2bb'b'' - ab^2 - a'b'^2 - a''b''^2 = 1,$$

zweitens, wodurch die Form bekanntlich als eine positive charakterisirt wird:

$$(14) \qquad A' = aa'' - b'^2 > 0.$$

Wählt man zu diesem Zwecke $b' = 1$, $b'' = 0$, so wird die Gleichung (13), wenn $A = a'a'' - b^2$ gesetzt wird,

$$(15) \qquad a' = aA - 1.$$

Kann man nun eine positive Zahl A nachweisen von der Beschaffenheit, dass $-A$ quadratischer Rest von a' ist, sodass die Congruenz

$$z^2 \equiv -A \pmod{a'}$$

auflösbar oder, was dasselbe ist, zwei ganze Zahlen b und a'' der Gleichung

$$A = a'a'' - b^2$$

gemäss angebbar sind, so wird, da $a > 1$ gedacht wird, a' und folglich nach Gleichung (13), der man die Gestalt

$$a'A' = ab^2 + 1$$

geben kann, auch A' positiv sein und die Form $\begin{pmatrix} a, & a', & a'' \\ b, & 1, & 0 \end{pmatrix}$ allen Bedingungen genügen. Eine solche Zahl A ist aber in der That nachweisbar.

Sei zuerst a von der Form $4n + 2$. Denkt man dann A positiv und von der Form $4n + 1$, so wird auch a' der Gleichung (15) zufolge von der Form $4n + 1$ und prim zu A und folglich

$$\left(\frac{-A}{a'}\right) = \left(\frac{A}{a'}\right) = \left(\frac{a'}{A}\right) = \left(\frac{-1}{A}\right) = 1.$$

Nun ist aber a' von der Form

$$a' = 4an + a - 1,$$

in welcher, dem Dirichlet'schen Satze von der arithmetischen Progression gemäss, jedenfalls eine positive Primzahl a' enthalten ist, von welcher also dann, wie verlangt, $-A$ quadratischer Rest ist.

Sei zweitens a ungerade, aber nicht von der Form $8n+7$. Setzt man dann $A = 8m + \varepsilon$ und wählt, was auf zwiefache Weise möglich sein wird, ε aus der Reihe 1, 3, 5, 7 so, dass $aA \equiv 3 \pmod{4}$ wird, so wird

$$a' = aA - 1$$

gerade, jedoch nicht theilbar durch 4. Wird demgemäss

$$a' = 2\alpha'$$

gesetzt, wo α' ungerade, so folgt aus vorstehender Gleichung ohne Schwierigkeit

$$\left(\frac{-A}{\alpha'}\right) = -(-1)^{\frac{\alpha'+1}{2}\frac{A+1}{2} + \frac{A^2-1}{8}};$$

und indem man nun nach einander für a die verschiedenen Formen $8n+1, 3, 5$ wählt, findet man folgende Combinationen:

$$a = 8n+1,\quad A = 8m+3,\quad \alpha' = 4h+1,\quad \left(\frac{-A}{\alpha'}\right) = +1$$

$$\text{"}\quad,\quad A = 8m+7,\quad \alpha' = 4h+3,\quad \left(\frac{-A}{\alpha'}\right) = -1$$

$$a = 8n+3,\quad A = 8m+1,\quad \alpha' = 4h+1,\quad \left(\frac{-A}{\alpha'}\right) = +1$$

$$\text{"}\quad,\quad A = 8m+5,\quad \alpha' = 4h+3,\quad \left(\frac{-A}{\alpha'}\right) = +1$$

$$a = 8n+5,\quad A = 8m+3,\quad \alpha' = 4h+3,\quad \left(\frac{-A}{\alpha'}\right) = +1$$

$$\text{"}\quad,\quad A = 8m+7,\quad \alpha' = 4h+1,\quad \left(\frac{-A}{\alpha'}\right) = -1.$$

Man sieht demnach, dass in allen Fällen A so wählbar ist, dass die Bedingung:

$$\left(\frac{-A}{\alpha'}\right) = 1$$

erfüllt wird. Aus Gleichung (15) folgt aber

$$\alpha' = \frac{1}{2}(aA-1) = 4am + \frac{1}{2}(a\varepsilon - 1),$$

wo zugleich mit α' auch $\frac{1}{2}(a\varepsilon - 1)$ zu $4a$ prim sein muss.

In dieser arithmetischen Progression findet sich somit auch eine positive Primzahl α' und in Bezug auf diese, ebenso aber dann auch in Bezug auf $a' = 2\alpha'$ wird $-A$, wie es sein soll, quadratischer Rest sein*).

7. Aus dem solcherweise bewiesenen Satze ziehen wir sogleich noch ein paar weitere Folgerungen.

Ist zunächst

$$4n + 2 = x^2 + x'^2 + x''^2,$$

so müssen nothwendig zwei der Zahlen x, x', x'', etwa die beiden ersten ungerade, die dritte gerade sein; setzen wir demgemäss

$$x = y + y', \quad x' = y - y', \quad x'' = 2y'',$$

so ergiebt sich unmittelbar

$$2n + 1 = y^2 + y'^2 + 2y''^2$$

d. h. der Satz: Jede ungerade Zahl ist als Summe von zwei einfachen und einem doppelten Quadrate darstellbar.

Ist ferner

$$8n + 3 = x^2 + x'^2 + x''^2,$$

so müssen alle drei Zahlen x, x', x'' ungerade, also

$$x = 2y + 1, \quad x' = 2y' + 1, \quad x'' = 2y'' + 1$$

sein, woraus dann sofort die Gleichung

$$n = \frac{y(y+1)}{2} + \frac{y'(y'+1)}{2} + \frac{y''(y''+1)}{2}$$

d. i. folgender Satz hervorgeht: Jede ganze Zahl lässt sich als Summe von drei Trigonalzahlen darstellen**).

---

*) Dirichlet zeigt a. a. O., dass dasselbe Verfahren auch noch in anderen Fällen, z. B. anwendbar ist, um nachzuweisen, dass jede durch 3 nicht theilbare Zahl in der Form $x^2 + x'^2 + 3x''^2$ eigentlich darstellbar ist. Nach derselben Methode hat Lebesgue (in Liouv. Journal des Mathém. 2. série, t. 2 p. 149) bewiesen, dass jede ungerade Zahl als Summe von vier Quadraten, deren zwei einander gleich sind, d. h. in der Form $x^2 + x'^2 + 2x''^2$ eigentlich darstellbar ist.

**) Bezeichnet man Trigonalzahlen zur Abkürzung mit $\Delta, \Delta', \Delta''$, so ist dem Satze zufolge jede ganze Zahl in der Form

$$n = \Delta + \Delta' + \Delta''$$

darstellbar. Aus

Von diesem Satze, der, wie der vorhergehende, in einem allgemeineren, von **Fermat** angegebenen Theoreme enthalten ist, gab **Lagrange** den ersten Beweis, der dann von **Euler** sehr vereinfacht worden ist*). Derselbe ruht auf ganz anderer Grundlage, als der hier gegebene, und stützt sich auf folgende drei Momente: erstens wird gezeigt, dass es für jede gegebene Primzahl p eine Summe von vier Quadraten giebt, welche theilbar ist durch p; zweitens wird hieraus gefolgert, dass p als Summe von vier Quadraten darstellbar ist, und drittens, dass dasselbe dann auch von jeder beliebigen Zahl gelten muss.

Den ersten, wichtigsten Punkt erledigen wir, indem wir, uns zum Theil auf **Euler's** Betrachtungen stützend, einen Satz beweisen, den **Lagrange** zum Ausgangspunkte nimmt. Er lautet folgendermassen: Ist p eine ungerade Primzahl, durch welche A und B nicht theilbar sind, so können drei ganze, nicht sämmtlich durch p theilbare Zahlen x, y, z so gewählt werden, dass der Ausdruck

$$x^2 + Ay^2 + Bz^2 \tag{16}$$

durch p aufgeht. Denn, wäre dies unrichtig, so würde $-A$ nothwendig ein quadratischer Nichtrest von p sein, weil sonst für ein passendes x

$$x^2 + A \cdot 1^2 + B \cdot 0^2 \equiv 0 \pmod{p}$$

wäre; dasselbe gilt von $-B$. Nun sei zuerst p von der Form $4n+1$ und b ein beliebiger Nichtrest von p, dann darf man

$$-Ab \equiv \alpha^2, \quad -Bb \equiv \beta^2$$

setzen, wodurch

$$b(x^2 + Ay^2 + Bz^2) \equiv bx^2 - (\alpha y)^2 - (\beta z)^2$$

also durch p theilbar wird, wenn man $x \equiv 0$ und, was bekanntlich für eine Primzahl p von der Form $4n+1$ möglich ist,

$$(\alpha y)^2 + (\beta z)^2 \equiv 0 \pmod{p}$$

wählt; also wird dann auch, gegen die Voraussetzung, der

---

*) **Lagrange** in den Mém. de l'Académie de Berlin 1770; **Euler** in den Acta Petrop. I, II 1775; s. auch Commentationes Arithmeticae collectae I S. 538: novae demonstrationes circa resolutionem numerorum in quadrata.

Ausdruck (16) durch p aufgehen. — Ist aber **zweitens** p von der Form $4n+3$, so werden A und B quadratische Reste von p also etwa

$$B \equiv y^2, \quad A \equiv z^2 \pmod{p}$$

sein, woraus

$$Ay^2 + Bz^2 \equiv 2AB$$

folgt; mithin muss $2AB$ und folglich $2A$ ein quadratischer Rest sein, denn sonst wäre $-2AB$ ein solcher, also

$$x^2 \equiv -2AB$$

und

$$x^2 + Ay^2 + Bz^2 \equiv 0 \pmod{p}$$

gegen die Annahme. Ist aber $2A$ ein quadratischer Rest, so hätte man Congruenzen von der Form

$$B \equiv y^2, \quad 2A \equiv z^2,$$

woraus

$$Ay^2 + Bz^2 \equiv 3AB$$

und weiter auf gleiche Weise wie vorher $3A$ als ein quadratischer Rest hervorgehen würde, u. s. w. Aber die Zahlen A, $2A$, $3A$, ... geben sämmtliche Reste (mod. p), unter denen es nicht **nur** quadratische **Reste** giebt, und man kommt also auch im jetzigen Falle auf einen Widerspruch.

Setzt man nun insbesondere $A = B = 1$, so erkennt man, dass es stets Zahlen x, y, z giebt, die nicht sämmtlich durch p aufgehen und für welche $x^2 + y^2 + z^2$*) oder auch allgemeiner eine Summe von vier Quadratzahlen:

$$x^2 + y^2 + z^2 + u^2$$

durch p theilbar ist. Nachdem dieser **erste** Punkt festgestellt

*) Diese Thatsache lässt sich nach **Hermite** (**Crelle's** Journal Bd. 47 S. 343) einfach folgendermassen erhärten: Setzt man $p \equiv \varepsilon$ (mod. 4), wo also ε gleich $+1$ oder -1 ist, so enthält die arithmetische Progression

$$4pz + 2\varepsilon p - 1$$

offenbar nur Zahlen von der Form $4n+1$; ausserdem aber ist $2\varepsilon p - 1$ prim zu $4p$, und demnach enthält sie auch eine **Primzahl** q jener Form, welche dann bekanntlich als Summe zweier Quadratzahlen darstellbar ist, also

$$4pz + 2\varepsilon p - 1 = x^2 + y^2$$

oder

$$x^2 + y^2 + 1^2 \equiv 0 \pmod{p}.$$

worden, begründet sich der zweite folgendermassen. In der Gleichung

$$(17) \qquad x^2 + y^2 + z^2 + u^2 = p \cdot P$$

darf man $P < p$ voraussetzen. Denn, wäre dies noch nicht der Fall, so zieht man für irgend welche ganze Zahlen ξ, η, ζ, v aus derselben die andere:

$$(x - \xi p)^2 + (y - \eta p)^2 + (z - \zeta p)^2 + (u - vp)^2 = p \cdot P',$$

in welcher nun, da x, y, z, u nicht sämmtlich durch p aufgehen, ξ, η, ζ, v so gewählt werden können, dass die Quadrate, ohne sämmtlich zu verschwinden, kleiner als $\frac{p^2}{4}$, P' also eine positive ganze Zahl $< p$ wird. Indem also von vornherein $P < p$ vorausgesetzt wird, liefert die Gleichung (17), falls $P = 1$ ist, eine Darstellung von p als Summe von vier Quadratzahlen, entgegengesetzten Falls darf man weiter annehmen, dass nicht sämmtliche Quadrate durch P theilbar sind, denn sonst erhielte man, falls P eine Quadratzahl ist, sogleich wieder eine Darstellung von p als Summe von vier Quadraten, andernfalls müsste p theilbar sein durch einen Faktor von P, was der Annahme, dass $P < p$, widerspricht. Nunmehr aber liefert die Gleichung (17) für irgend welche ganze Zahlen ξ, η, ζ, v die andere:

$$(x - P\xi)^2 + (y - P\eta)^2 + (z - P\zeta)^2 + (u - Pv)^2 = P \cdot Q$$

und man kann über jene Zahlen so verfügen, dass jedes der Quadrate, ohne dass sie sämmtlich verschwinden, kleiner als $\frac{P^2}{4}$ und somit $Q < P$ wird. Multiplicirt man nun mit Hilfe der Formel (22) des ersten Capitels, indem man in derselben

$$x, \; -y, \; -z, \; -u \quad \text{statt } \xi, x, x', x'',$$

$$x - P\xi, \; y - P\eta, \; z - P\zeta, \; u - Pv \quad \text{statt } \eta, y, y', y''$$

setzt, die vorige Gleichung mit der Gleichung (17), so findet man sogleich, dass die vier Quadrate, aus denen die linke Seite sich zusammensetzt, durch P^2 theilbar werden, und somit folgende Gleichung:

$$(p - x\xi - y\eta - z\zeta - uv)^2 + (x\eta - y\xi - u\zeta + zv)^2$$
$$+ (x\zeta - z\xi - yv + u\eta)^2 + (xv - u\xi + y\zeta - z\eta)^2 = p \cdot Q.$$

Dies ist eine Gleichung von der Gestalt der Gleichung (17), aber es ist $Q < P$. Da hiernach Q auch $< p$ ist, können wieder nicht sämmtliche Quadrate durch Q theilbar sein, und folglich kann man auf ähnliche Weise weiter fortgehen u. s. w. und muss so endlich zu einer Gleichung derselben Form gelangen, deren rechte Seite p selbst ist, d. i. zu einer Darstellung der ungeraden Primzahl p als Summe von vier Quadratzahlen.

Dass die einzige gerade Primzahl 2 gleichfalls so darstellbar ist, bedarf keines Beweises, es ist

$$1^2 + 1^2 + 0^2 + 0^2 = 2.$$

Ist aber jede Primzahl so darstellbar, so folgt drittens ohne weiteres aus der angezogenen Formel des ersten Capitels, dass auch jede beliebige Zahl als eine Summe von vier Quadratzahlen dargestellt werden kann*).

Wie gross die Anzahl solcher Darstellungen ist, wird später ermittelt werden (zweiter Abschnitt, zehntes Capitel).

8. Wir wenden uns nunmehr zu dem allgemeinen Fermat'schen Theoreme, dessen wir bereits gedachten und von welchem die beiden Sätze von den Trigonalzahlen und den vier Quadratzahlen nur die beiden einfachsten Fälle sind. Dieses schöne Theorem behauptet: Jede positive ganze Zahl kann als Summe von n (oder weniger) Polygonalzahlen n^{ter} Ordnung dargestellt werden. Fermat hat leider seinen Satz nur ausgesprochen, ohne von seiner Beweis-

*) Vgl. hierzu noch die Sätze von Lionnet, welche Lebesgue (Nouv. Ann. 2. sér. 11, p. 516) aus der Zerlegung der Zahlen in die Summe dreier Quadrate hergeleitet hat, sowie auch Realis (ebendas. 2. sér. 12 p. 212), wo Darstellungen von Zahlen als Summe von vier Quadraten nachgewiesen werden, bei denen die Grundzahlen der Quadrate gewisse Bedingungen erfüllen. Ferner sei auf Liouville's Notiz in s. Journal 2. sér. 1 p. 230 über die Darstellbarkeit der Zahlen durch die Form

$$x^2 + ay^2 + bz^2 + abu^2$$

sowie auf die Unmenge von Sätzen, die er in späteren Bänden desselben Journals über die Darstellbarkeit durch besondere quadratische Formen mit vier Veränderlichen (ohne Beweis) gegeben hat, hier verwiesen.

methode irgend welche Andeutung zu geben. Erst Cauchy*) gelang es, einen aus sehr einfachen Betrachtungen geschöpften, wenn auch umständlichen Beweis dafür zu erbringen, welchen Legendre mit mancherlei Modifikationen, die zu seiner Vereinfachung dienen sollen, in der dritten Ausgabe seiner théorie des nombres (t. 2, sixième partie) wiederholt hat; auch gab Cauchy dem Satze eine noch bestimmtere Fassung, indem er ihn in folgender Form aufstellte:

Jede positive ganze Zahl kann als Summe von $m+2$ Polygonalzahlen $m+2^{\text{ter}}$ Ordnung dargestellt werden, von welchen $m-2$ gleich 0 oder 1 sind.

Wir wollen versuchen, seinen Beweis hier möglichst einfach darzustellen.

Zunächst sei an die Definition der Polygonalzahlen erinnert. Sind

$$1,\ m+1,\ 2m+1,\ \cdots (\mu-1)m+1$$

die ersten μ Glieder einer arithmetischen Reihe mit dem Anfangsgliede 1 und der Differenz m, so heisst die Summe derselben, nämlich

$$m \cdot \frac{\mu(\mu-1)}{2} + \mu, \tag{18}$$

eine Polygonalzahl $m+2^{\text{ter}}$ Ordnung. Für $m=1$ erhält man die Trigonalzahlen $\frac{\mu(\mu+1)}{2}$, für $m=2$ die Quadratzahlen μ^2. Der Definition gemäss wird μ als eine nicht-negative ganze Zahl vorausgesetzt werden, obwohl man das in der Formel (18) enthaltene Bildungsgesetz auch auf die negativen Werthe von μ ausdehnen darf, wodurch, wenigstens wenn $m > 2$, zwei verschiedene Reihen von Polygonalzahlen hervorgehen werden. Im Fermat'schen Satze sind jedoch nur Zahlen derjenigen Reihe gemeint, welche nicht-negativen Werthen von μ entspringen. In jeder Ordnung dieser Polygonalzahlen kommen dann die beiden Zahlen 0 und 1 vor, welche in der That aus (18) entstehen, wenn man $\mu = 0$ resp. $\mu = 1$ wählt.

---

*) Cauchy's Abhandlung wurde der Pariser Akademie am 13. Novb. 1815 vorgelegt.

Nach diesen Vorbemerkungen wird daher der Fermat'sche Satz in der Fassung von Cauchy auch folgendermassen ausgedrückt werden können: Ist N eine positive ganze Zahl, so kann man

$$N = \left(m \cdot \frac{t^2 - t}{2} + t\right) + \left(m \cdot \frac{u^2 - u}{2} + u\right) + \left(m \cdot \frac{v^2 - v}{2} + v\right) + \left(m \cdot \frac{w^2 - w}{2} + w\right) + r \tag{19}$$

setzen, während r eine bestimmte Zahl der Reihe

$$0, 1, 2, \cdots m - 2,$$

t, u, v, w aber nicht-negative ganze Zahlen sind.

Es gilt also zu zeigen, dass N in der Gestalt

$$N = \frac{m}{2}(x - s) + s + r \tag{20}$$

dargestellt werden kann, wo r eine Zahl der Reihe $0, 1, 2, \ldots m - 2$; x und s aber nicht-negative ganze Zahlen sind, welche eine gleichzeitige Darstellung mittels nicht-negativer ganzer Zahlen t, u, v, w gemäss den Gleichungen

$$\begin{cases} x = t^2 + u^2 + v^2 + w^2 \\ s = t + u + v + w \end{cases} \tag{21}$$

gestatten. Man sieht sogleich aus dem Umstande, dass

$$x^2 + x = x(x + 1)$$

stets eine gerade Zahl ist, dass auch $x + s$ eine solche und folglich x und s gleichartige Zahlen, beide gerade oder beide ungerade sein müssen. Auch folgt aus der Identität

$$4(t^2 + u^2 + v^2 + w^2)$$
$$= (t + u + v + w)^2 + (t + u - v - w)^2 + (t - u + v - w)^2 + (t - u - v + w)^2,$$

dass

$$4x - s^2 > 0$$

sein muss, also $s < \sqrt{4x}$. Diese beiden Bedingungen, welche die Zahlen x und s erfüllen müssen, reichen nun zwar zur Möglichkeit ihrer Darstellung gemäss den Gleichungen (21) nicht aus. Aber man kann folgenden Satz beweisen: Ist x eine ungerade und s eine zwischen $\sqrt{3x - 2} - 1$ und

$\sqrt{4\varkappa}$ enthaltene gleichfalls ungerade Zahl, so giebt es nicht-negative ganze Zahlen t, u, v, w, welche die Gleichungen (21) erfüllen.

1) Um diesen Satz zu beweisen, bemerken wir erstens, dass, so oft x, y, z nicht-negative Zahlen sind, zufolge der Ungleichheiten

$$(x + y + z)^2 \overline{\gtrless} x^2 + y^2 + z^2$$

$$(x + y + z)^2 \overline{\lessgtr} (x + y + z)^2 + (y - z)^2 + (z - x)^2 + (x - y)^2$$

aus einer Gleichheit

$$x^2 + y^2 + z^2 = a$$

sogleich die Ungleichheiten

$$\sqrt{a} \overline{\lessgtr} x + y + z \overline{\lessgtr} \sqrt{3a} \tag{22}$$

sich ergeben.

2) Sei nun $\varkappa$ eine ungerade Zahl und s eine zwischen $\sqrt{3\varkappa - 2} - 1$ und $\sqrt{4\varkappa}$ enthaltene gleichfalls ungerade Zahl. Da alsdann $4\varkappa - s^2$ von der Form $8n + 3$ ist, giebt es nach dem Satze in nr. 6 positive ungerade Zahlen x, y, z von der Beschaffenheit, dass

$$4\varkappa - s^2 = x^2 + y^2 + z^2$$

oder

$$4\varkappa = x^2 + y^2 + z^2 + s^2 \tag{23}$$

ist. Da ferner $\sqrt{3\varkappa - 2} - 1 < s$, also $3\varkappa < s^2 + 2s + 3$ ist, folgt nach (22), wenn man $a = 4\varkappa - s^2$ wählt,

$$x + y + z < \sqrt{s^2 + 8s + 12} < s + 4.$$

Bildet man daher die acht Zahlen

$$\frac{s \pm x \pm y \pm z}{4},$$

entsprechend den verschiedenen möglichen Combinationen der Vorzeichen, so ist die algebraisch kleinste von ihnen,

$$\frac{s - x - y - z}{4},$$

noch algebraisch > -1, und demnach werden sie, falls sie ganze Zahlen sind, Null oder positiv sein müssen. Nun sind die beiden Zahlen

$$s + x + y + z, \quad s - x - y - z,$$

da s, x, y, z ungerade sind, gerade Zahlen und ihr Unter-

schied congruent 2 (mod. 4), also ist eine von ihnen theilbar durch 4, mithin entweder

$$t = \frac{s + x + y + z}{4}$$

eine ganze Zahl und dann sind auch

$$u = \frac{s + x - y - z}{4}, \quad v = \frac{s - x + y - z}{4}, \quad w = \frac{s - x - y + z}{4}$$

ganze Zahlen; oder

$$t = \frac{s - x - y - z}{4}$$

ist eine ganze Zahl, und dann sind auch

$$u = \frac{s - x + y + z}{4}, \quad v = \frac{s + x - y + z}{4}, \quad w = \frac{s + x + y - z}{4}$$

ganze Zahlen. In beiden Fällen aber findet man

$$t + u + v + w = s$$

und

$$t^2 + u^2 + v^2 + w^2 = \frac{1}{4}(s^2 + x^2 + y^2 + z^2) = \varkappa.$$

Man erkennt hieraus die Richtigkeit des ausgesprochenen Satzes.

3) Vor Allem ist nun weiter zu bemerken, dass zwischen den Grenzen

$$\sqrt{3\varkappa - 2} - 1 \quad \text{und} \quad \sqrt{4\varkappa}$$

stets eine mit $\varkappa$ gleichartige Zahl s vorhanden ist. Man bestätigt dies leicht durch den Versuch für die Zahlen $\varkappa \overline{\gtrless} 9$, für $\varkappa > 9$ folgt es allgemein aus dem Umstande, dass dann, wie sehr einfach zu erkennen, die Differenz

$$\sqrt{4\varkappa} - (\sqrt{3\varkappa - 2} - 1) > 2$$

ist, zwischen diesen Grenzen also mindestens zwei aufeinanderfolgende ganze Zahlen enthalten sind. Für $\varkappa = 121$ wird die Differenz sogar gleich 4 und bleibt für alle $\varkappa > 121$ grösser als 4; für diese Werthe von $\varkappa$ liegen also zwischen den angegebenen Grenzen mindestens vier aufeinanderfolgende, gewiss also mindestens zwei mit $\varkappa$ gleichartige ganze Zahlen und ebenso mindestens zwei mit $\varkappa$ ungleichartige. Gesetzt daher, für eine ungerade Zahl $\varkappa$ fände sich zwischen den Grenzen

$$\sqrt{3(\varkappa + 1) - 2} - 1 \quad \text{und} \quad \sqrt{4(\varkappa + 1)}$$

nur eine ungerade Zahl s, so muss $x + 1 < 121$ sein. Solcher Zahlen x giebt es mithin nur eine mässig grosse endliche Anzahl, und man kann — wovon Cauchy durch eine ganze Reihe von Sätzen den strengen Nachweis bringt — sich durch den Versuch davon überzeugen, dass man für jede dieser ungeraden Zahlen x und die zugehörige ungerade Zahl s *einem* der beiden folgenden Systeme von Gleichungen durch nicht-negative ganze Zahlen t, u, v, w Genüge leisten kann:

$$(24)\quad \left\{\begin{array}{l} \text{entweder:} \\ \quad x + 1 = t^2 + u^2 + v^2 + w^2 \\ \quad s - 1 = t + u + v + w \\ \text{oder} \\ \quad x + 1 = t^2 + u^2 + v^2 + w^2 \\ \quad s + 1 = t + u + v + w. \end{array}\right.$$

4) Nachdem auch dieser Punkt festgestellt worden, denke man sich für eine ungerade Zahl x sämmtliche verschiedene ungerade Zahlen, die zwischen den Grenzen

$$\sqrt{3x - 2} - 1 \quad \text{und} \quad \sqrt{4x}$$

enthalten sind, und nenne s_1 die kleinste, s_2 die grösste von ihnen, indem man $s_1 = s_2$ setzt, sobald etwa nur eine solche Zahl dazwischen enthalten ist. Indem man in dem Ausdrucke

$$(25)\qquad A_x = m \cdot \frac{x - s}{2} + s + r$$

sowohl für r alle seine zulässigen Werthe

$$0, 1, 2, \cdots m - 2,$$

als auch für s die Werthe

$$s_1, s_1 + 2, s_1 + 4, \cdots s_2$$

einsetzt, erkennt man leicht, dass der kleinste aller so entstehenden Werthe der Werth

$$(26)\qquad B_x = m \cdot \frac{x - s_2}{2} + s_2,$$

der grösste aber der Werth

$$(27)\qquad C_x = m \cdot \frac{x - s_1}{2} + s_1 + m - 2$$

ist; denn man findet nach den Voraussetzungen

$$A_x - B_x = \left(\frac{m}{2} - 1\right) \cdot (s_2 - s) + r \gtreqless 0$$

$$C_x - A_x = \left(\frac{m}{2} - 1\right) \cdot (s - s_1) + m - 2 - r \gtreqless 0,$$

da $m > 2$ angenommen werden darf. Die verschiedenen Werthe des Ausdrucks A_x bilden aber die gesammte Reihe aller ganzen Zahlen von B_x bis C_x, sodass jede Zahl N dieser Reihe in die Gestalt

$$N = \frac{m}{2}(x - s) + s + r$$

gesetzt werden kann. In der That, jene Werthe sind der Reihe nach die folgenden:

$$\frac{m}{2}(x - s_2) + s_2, \quad \frac{m}{2}(x - s_2) + s_2 + 1, \cdots$$
$$\cdots \frac{m}{2}(x - s_2) + s_2 + m - 2$$

$$\frac{m}{2}(x - s_2 + 2) + s_2 - 2, \quad \frac{m}{2}(x - s_2 + 2) + s_2 - 1, \cdots$$
$$\cdots \frac{m}{2}(x - s_2 + 2) + s_2 + m - 4$$

$$\frac{m}{2}(x - s_2 + 4) + s_2 - 4, \quad \frac{m}{2}(x - s_2 + 4) + s_2 - 3, \cdots$$
$$\cdots \frac{m}{2}(x - s_2 + 4) + s_2 + m - 6$$

. . . .

$$\frac{m}{2}(x - s_1) + s_1, \quad \frac{m}{2}(x - s_1) + s_1 + 1, \cdots$$
$$\cdots \frac{m}{2}(x - s_1) + s_1 + m - 2,$$

und man sieht, wie jedes erste Glied einer Reihe dem letzten der vorangehenden gleich ist, mithin die Glieder vom ersten an, welches B_x ist, die aufeinanderfolgenden ganzen Zahlen darstellen bis zum letzten, welches C_x ist. — Verbindet man dies Resultat nun mit dem zuvor bewiesenen Satze, (unter 2)), so darf man sogleich schliessen: Jede Zahl zwischen den Grenzen B_x und C_x inclusive lässt sich als Summe von $m + 2$ Polygonalzahlen $m + 2^{\text{ter}}$ Ordnung darstellen, von denen $m - 2$ gleich 0 oder 1 sind.

5) Hierdurch ist der Satz von Fermat für alle Zahlen des Intervalls von $B_\varkappa$ bis $C_\varkappa$ bewiesen. Aber $\varkappa$ ist jede beliebige ungerade Zahl; demnach wird der Satz auch Geltung haben für das Intervall von $B_{\varkappa+2}$ bis $C_{\varkappa+2}$, wenn man

$$(26a)\qquad B_{\varkappa+2} = \frac{m}{2}(\varkappa + 2 - s_2') + s_2'$$

$$(27a)\qquad C_{\varkappa+2} = \frac{m}{2}(\varkappa + 2 - s_1') + s_1' + m - 2$$

setzt und dabei unter s_1', s_2' die kleinste und die grösste der ungeraden Zahlen versteht, welche zwischen den Grenzen

$$\sqrt{3(\varkappa+2)-2} - 1 \quad \text{und} \quad \sqrt{4(\varkappa+2)}$$

enthalten sind. Nun ist sowohl der Unterschied

$$(\sqrt{3(\varkappa+2)-2} - 1) - (\sqrt{3\varkappa-2} - 1)$$

als auch der Unterschied

$$\sqrt{4(\varkappa+2)} - \sqrt{4\varkappa},$$

wie leicht ersichtlich, kleiner als 2, und folglich kann s_1' nur entweder gleich s_1 oder gleich $s_1 + 2$ und ebenso s_2' nur entweder gleich s_2 oder gleich $s_2 + 2$ sein. Aus (27a) folgt hiernach sogleich $C_{\varkappa+2} \overline{\gtrless} C_\varkappa + 2$; da aber dasselbe Räsonnement beliebig oft wiederholt werden kann, sieht man, dass die Reihe der analog gebildeten Zahlen $C_\varkappa, C_{\varkappa+2}, C_{\varkappa+4}, \ldots$ mit wachsendem Index über jede Grenze hinauswächst.

6) Ist nun erstens $s_2' - s_1 \overline{\gtrless} 2$, so folgt leicht aus (26a)

$$B_{\varkappa+2} \overline{\overline{<}} C_\varkappa + 1;$$

weil aber der Satz von Fermat für jede zwischen $B_{\varkappa+2}$ und $C_{\varkappa+2}$ inclusive enthaltene ganze Zahl schon erwiesen ist, so gilt er a fortiori für jede zwischen $C_\varkappa + 1$ und $C_{\varkappa+2}$ inclusive, und, weil er auch für $C_\varkappa$ richtig ist, für jede zwischen $C_\varkappa$ und $C_{\varkappa+2}$ enthaltene Zahl. Mit Beachtung des in 4) Bewiesenen folgt hieraus offenbar: Der Fermat'sche Satz gilt für jede ganze Zahl zwischen $B_\varkappa$ und $C_{\varkappa+2}$.

Ist zweitens aber $s_2' - s_1 = 0$ d. h. nur eine einzige ungerade Zahl zwischen den Grenzen

$$\sqrt{3\varkappa-2} - 1 \quad \text{und} \quad \sqrt{4(\varkappa+2)}$$

also auch nur zwischen den engeren Grenzen

$$\sqrt{3(x+1)-2}-1 \quad \text{und} \quad \sqrt{4(x+1)}$$

enthalten, so besteht für $s = s_1$ nach 3) eins der beiden Gleichungssysteme (24) und gleichzeitig wird

$$B_{x+2} = C_x + 2.$$

Da nun der Satz von Fermat im Intervalle von B_{x+2} bis C_{x+2}, jedoch auch für C_x schon erwiesen ist, so ist er im Intervalle von C_x bis C_{x+2} für die einzige Zahl $C_x + 1$ noch fraglich. Diese Zahl jedoch, nämlich die Zahl

$$m \cdot \frac{x-s_1}{2} + s_1 + m - 1,$$

nimmt, je nachdem von den beiden Gleichungssystemen (24) das erste oder das zweite gilt, entweder die Form

$$\left(m \cdot \frac{t^2-t}{2} + t\right) + \left(m \cdot \frac{u^2-u}{2} + u\right) + \left(m \cdot \frac{v^2-v}{2} + v\right) + \left(m \cdot \frac{w^2-w}{2} + w\right)$$

oder dieselbe Form $+ m - 2$ an und gehorcht somit dem Fermat'schen Satze. Man findet also auch im gegenwärtigen Falle, dass dieser Satz für jede ganze Zahl zwischen B_x und C_{x+2} besteht.

Wegen 5) schliesst man nun offenbar: derselbe Satz gilt für jede ganze Zahl, welche gleich oder grösser ist als B_x. Nimmt man endlich für x die ungerade Zahl 1, für welche B_x ebenfalls gleich 1 wird, so erschliesst man aus dem Bewiesenen die Giltigkeit des Fermat'schen Satzes von den Polygonalzahlen genau in der Fassung, welche Cauchy ihm gegeben, für jede positive ganze Zahl. —

Legendre hat diesem Satze noch eine Reihe von specielleren Sätzen hinzugefügt, aus welchen hervorgeht, dass über eine gewisse, für jede Ordnung der Polygonalzahlen leicht angebbare Grenze hinaus jede Zahl sich in vier, höchstens fünf Polygonalzahlen zerlegen lässt. Hier mag es genügen, auf diese weiteren Sätze über Polygonalzahlen noch hingewiesen zu haben*).

*) Legendre, théorie des nombres 3. éd.

Siebentes Capitel.

Bestimmung des Maasses eines Geschlechts und einer Ordnung positiver Formen.

1. Von der besonderen Form $x^2 + x'^2 + x''^2$ wenden wir uns zur Betrachtung der positiven Formen überhaupt wieder zurück, um jetzt allgemein das Maass zunächst eines Geschlechts solcher Formen zu ermitteln. Eisenstein, dem man die Einführung dieses Begriffs verdankt, hat auch bereits eine Reihe von Formeln angegeben*), die zur Bestimmung des Maasses eines Geschlechts oder einer Ordnung dienen. In seiner vortrefflichen Arbeit „Vergleichung von solchen ternären quadratischen Formen, welche verschiedene Determinanten haben" in den Monatsber. der Berl. Akad. v. J. 1852 berichtet er, dass er zu seinen Resultaten geführt worden sei, als er sich vergeblich bemüht habe, die scheinbar weit näher liegende Aufgabe: die Bestimmung der Classenanzahl, zu lösen.

Inwieweit er dabei der Dirichlet'schen Methoden sich bedient haben mag, geht aus seinen Angaben nicht klar hervor**), und so kann man auf seine Herleitung der erwähnten Formeln nur aus der Methode schliessen, die er in der eben angeführten Arbeit v. J. 1852 ausführlich dargestellt hat, eine Methode, welche ausser dem Interesse, das sie an sich gewährt, darum Aufmerksamkeit verdient, weil sie nur ganz elementarer Hilfsmittel bedarf.

Ihrer Darstellung müssen einige allgemeine Betrachtungen über lineare Substitutionen voraufgeschickt werden, die ebenfalls zuerst Eisenstein verwendet hat***); es genüge, sie

---

*) S. seine Arbeit „Neue Theoreme der höheren Arithmetik" in Crelle's Journal f. d. r. u. a. Math. Bd. 35, sowie die Abhandlung „Tabelle der reducirten pos. ternären quadrat. Formen u. s. w." ebendas. Bd. 41; die letztere ist auch als ein besonderes Werkchen 1851 bei Reimer, Berlin, erschienen.

**) S. den Schluss seiner Arbeit „Neue Theoreme u. s. w."

***) Im § 6 seiner Abhandlung „Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln u. s. w." in Crelle's Journal Bd. 28 S. 328 und 330.

hier für den Fall dreier Variabeln zu entwickeln, doch gelten sie, wie leicht zu übersehen, für jede Anzahl derselben. —

Sei

$$(1)\qquad \begin{cases} x = \alpha y + \beta y' + \gamma y'' \\ x' = \alpha' y + \beta' y' + \gamma' y'' \\ x'' = \alpha'' y + \beta'' y' + \gamma'' y'' \end{cases}$$

eine Substitution S mit dem positiven Modulus M und T irgend eine Substitution

$$(2)\qquad \begin{cases} y = \lambda z + \mu z' + \nu z'' \\ y' = \lambda' z + \mu' z' + \nu' z'' \\ y'' = \lambda'' z + \mu'' z' + \nu'' z'' \end{cases}$$

mit dem Modulus 1, so wird der Modulus der zusammengesetzten Substitution $U = S \cdot T$ gleich M sein. Die sämmtlichen, aus S durch Zusammensetzung mit den sämmtlichen unimodularen Substitutionen T entstehenden Substitutionen U nennt Eisenstein die Classe der mit S äquivalenten Substitutionen, wobei sogleich einleuchtet, dass diese Classe unverändert bleibt, wenn man S durch irgend eine andere Substitution ihrer Classe ersetzt. Es soll nun gezeigt werden, dass es für jede gegebene Substitution S eine einzige, völlig bestimmte Substitution T giebt von der Beschaffenheit, dass die zusammengesetzte Substitution U die Form hat:

$$(3)\qquad U = \begin{pmatrix} \delta, & 0 & 0 \\ \varepsilon', & \delta', & 0 \\ \eta'', & \theta'', & \delta'' \end{pmatrix}$$

wo $\delta, \delta', \delta''$ positive ganze Zahlen sind, deren Produkt gleich M ist, während $\varepsilon', \eta'', \theta''$ den Bedingungen genügen, dass

$$(4)\qquad 0 \overline{\gtrless} \varepsilon' < \delta', \quad 0 \overline{\gtrless} \begin{Bmatrix} \theta'' \\ \eta'' \end{Bmatrix} < \delta''.$$

Nennt man eine solche Substitution mit Eisenstein eine reducirte Substitution vom Modulus M, so kann man die Behauptung auch so aussprechen: in jeder Classe äquivalenter Substitutionen giebt es stets eine einzige reducirte Substitution.

Um dies nachzuweisen, stellen wir vor allem die zusammengesetzte Substitution auf:

$$(5)\quad \begin{cases} x = (\alpha\lambda + \beta\lambda' + \gamma\lambda'')z + (\alpha\mu + \beta\mu' + \gamma\mu'')z' \\ \qquad + (\alpha\nu + \beta\nu' + \gamma\nu'')z'' \\ x' = (\alpha'\lambda + \beta'\lambda' + \gamma'\lambda'')z + (\alpha'\mu + \beta'\mu' + \gamma'\mu'')z' \\ \qquad + (\alpha'\nu + \beta'\nu' + \gamma'\nu'')z'' \\ x'' = (\alpha''\lambda + \beta''\lambda' + \gamma''\lambda'')z + (\alpha''\mu + \beta''\mu' + \gamma''\mu'')z' \\ \qquad + (\alpha''\nu + \beta''\nu' + \gamma''\nu'')z''. \end{cases}$$

Bezeichnet nun δ den (positiven) grössten gemeinsamen Theiler von α, β, γ, so lassen sich ganze Zahlen $\lambda, \lambda', \lambda''$ so wählen, dass

$$\frac{\alpha}{\delta} \cdot \lambda + \frac{\beta}{\delta} \cdot \lambda' + \frac{\gamma}{\delta} \cdot \lambda'' = 1$$

wird, und, wenn $\lambda_0, \lambda_0', \lambda_0''$ eine Auflösung dieser Gleichung bedeutet, so ist ihre allgemeine Auflösung folgende:

$$(6)\quad \begin{cases} \lambda = \lambda_0 - i \cdot \frac{\gamma}{\delta} + k \cdot \frac{\beta}{\delta}, \quad \lambda' = \lambda_0' - k \cdot \frac{\alpha}{\delta} + h \cdot \frac{\gamma}{\delta}, \\ \lambda'' = \lambda_0'' - h \cdot \frac{\beta}{\delta} + i \cdot \frac{\alpha}{\delta}, \end{cases}$$

wenn h, i, k unbestimmte ganze Zahlen bedeuten. Sollen nun zuerst

$$\alpha\mu + \beta\mu' + \gamma\mu'' = 0, \quad \alpha\nu + \beta\nu' + \gamma\nu'' = 0$$

werden, so müssen

$$(7)\quad \mu'\nu'' - \mu''\nu' = \frac{\alpha}{\delta}, \quad \mu''\nu - \mu\nu'' = \frac{\beta}{\delta}, \quad \mu\nu' - \mu'\nu = \frac{\gamma}{\delta}$$

sein, Gleichungen, denen man nach dem Gauss'schen Hilfssatze stets genügen kann, und zwar ist, wenn $\mu_0, \mu_0', \mu_0'', \nu_0, \nu_0', \nu_0''$ eine Lösung derselben bilden, ihre allgemeine Auflösung durch die Formeln

$$\mu = m\mu_0 + r\nu_0, \quad \mu' = m\mu_0' + r\nu_0', \quad \mu'' = m\mu_0'' + r\nu_0''$$
$$\nu = n\mu_0 + s\nu_0, \quad \nu' = n\mu_0' + s\nu_0', \quad \nu'' = n\mu_0'' + s\nu_0''$$

gegeben, wenn die ganzen Zahlen m, n, r, s der Gleichung

$$(8)\quad ms - nr = 1$$

gemäss gewählt werden. Hieraus fliessen die Beziehungen

$$\begin{aligned}&\alpha'\mu + \beta'\mu' + \gamma'\mu'' \\ &= m(\alpha'\mu_0 + \beta'\mu_0' + \gamma'\mu_0'') + r(\alpha'\nu_0 + \beta'\nu_0' + \gamma'\nu_0'') \\ &\alpha'\nu + \beta'\nu' + \gamma'\nu'' \\ &= n(\alpha'\mu_0 + \beta'\mu_0' + \gamma'\mu_0'') + s(\alpha'\nu_0 + \beta'\nu_0' + \gamma'\nu_0'').\end{aligned}$$

Bedeutet nun δ' den (positiven) grössten gemeinsamen Theiler von

$$\alpha'\mu_0 + \beta'\mu_0' + \gamma'\mu_0'' \quad \text{und} \quad \alpha'\nu_0 + \beta'\nu_0' + \gamma'\nu_0'',$$

eine Zahl, welche den voraufgehenden Beziehungen gemäss von der besonderen Wahl der Lösung $\mu_0, \mu_0', \mu_0'', \nu_0, \nu_0', \nu_0''$ unabhängig ist, so wird man

$$\alpha'\nu + \beta'\nu' + \gamma'\nu'' = 0$$

machen, wenn man

$$n = -\frac{\alpha'\nu_0 + \beta'\nu_0' + \gamma'\nu_0''}{\delta'}, \quad s = \frac{\alpha'\mu_0 + \beta'\mu_0' + \gamma'\mu_0''}{\delta'}$$

wählt, und, bedeutet dann m_0, r_0 eine Lösung der Gleichung (8), so ist ihre allgemeine Lösung

$$m = m_0 + t \cdot n, \quad r = r_0 + t \cdot s,$$

und man findet einerseits

$$\alpha'\mu + \beta'\mu' + \gamma'\mu'' = \delta'$$

andererseits

$$\begin{aligned}&\alpha''\nu + \beta''\nu' + \gamma''\nu'' \\ &= n(\alpha''\mu_0 + \beta''\mu_0' + \gamma''\mu_0'') + s(\alpha''\nu_0 + \beta''\nu_0' + \gamma''\nu_0'') \\ &= \frac{1}{\delta'}\left[-(\alpha''\mu_0 + \beta''\mu_0' + \gamma''\mu_0'')(\alpha'\nu_0 + \beta'\nu_0' + \gamma'\nu_0'')\right. \\ &\qquad \left. + (\alpha'\mu_0 + \beta'\mu_0' + \gamma'\mu_0'')(\alpha''\nu_0 + \beta''\nu_0' + \gamma''\nu_0'')\right] \\ &= \frac{1}{\delta'}\big((\alpha'\beta'' - \alpha''\beta')(\mu_0\nu_0' - \mu_0'\nu_0) \\ &\quad + (\beta'\gamma'' - \beta''\gamma')(\mu_0'\nu_0'' - \mu_0''\nu_0') \\ &\quad + (\gamma'\alpha'' - \gamma''\alpha')(\mu_0''\nu_0 - \mu_0\nu_0'')\big) \\ &= \frac{M}{\delta\delta'}.\end{aligned}$$

Da der Ausdruck zur Linken aber eine ganze Zahl ist, welche δ'' heisse, so ergiebt sich M als das Produkt der drei Zahlen $\delta, \delta', \delta''$,

$$M = \delta \cdot \delta' \cdot \delta'' \tag{9}$$

und

$$\alpha''\nu + \beta''\nu' + \gamma''\nu'' = \delta''.$$

Ferner kommt

$$\alpha''\mu + \beta''\mu' + \gamma''\mu''$$
$$= m(\alpha''\mu_0 + \beta''\mu_0' + \gamma''\mu_0'') + r(\alpha''\nu_0 + \beta''\nu_0' + \gamma''\nu_0'')$$
$$= m_0(\alpha''\mu^0 + \beta''\mu_0' + \gamma''\mu_0'') + r_0(\alpha''\nu_0 + \beta''\nu_0' + \gamma''\nu_0'')$$
$$+ t \cdot \delta'',$$

wo nun über die ganze Zahl t in eindeutiger Weise so verfügt werden kann, dass

$$\alpha''\mu + \beta''\mu' + \gamma''\mu''$$

zwischen 0 inclusive und δ'' exclusive zu liegen kommt. Endlich nehmen die Ausdrücke (6) für $\lambda, \lambda', \lambda''$, wenn man

$$h\mu + i\mu' + k\mu'' = l'$$
$$h\nu + i\nu' + k\nu'' = l''$$

setzt, nachstehende Gestalt an:

$$\lambda = \lambda_0 - l''\mu + l'\nu, \quad \lambda' = \lambda_0' - l''\mu' + l'\nu',$$
$$\lambda'' = \lambda_0'' - l''\mu'' + l'\nu'',$$

in Folge wovon man findet:

$$\alpha'\lambda + \beta'\lambda' + \gamma'\lambda'' = \alpha'\lambda_0 + \beta'\lambda_0' + \gamma'\lambda_0'' - l''\cdot \delta',$$
$$\alpha''\lambda + \beta''\lambda' + \gamma''\lambda''$$
$$= \alpha''\lambda_0 + \beta''\lambda_0' + \gamma''\lambda_0'' - l''(\alpha''\mu + \beta''\mu' + \gamma''\mu'') + l' \cdot \delta''$$

Hier kann aber zunächst die ganze Zahl l'' auf eindeutige Weise so gewählt werden, dass der erstere dieser Ausdrücke, und sodann auf eindeutige Weise auch die ganze Zahl l' so, dass der zweite derselben zwischen die bei (4) angegebenen Grenzen zu liegen kommt, und somit ist das Behauptete vollständig erwiesen. —

Da andererseits die Substitution (3) für jedes der Werthsysteme $\delta, \delta', \delta'', \varepsilon', \eta'', \theta''$, welches die angegebenen Bedingungen erfüllt, eine Substitution vom Modulus M ist, so giebt es so viel reducirte Substitutionen mithin auch soviel Classen nicht äquivalenter Substitutionen vom Modulus M, als die Anzahl jener Werthsysteme beträgt, d. i. für jede Zerlegung $M = \delta \cdot \delta' \cdot \delta''$ genau $\delta'\delta''^2$, im Ganzen also

$$\sum \delta'\delta''^2,$$

die Summe auf alle Lösungen der Gleichung (9) bezogen.

Besteht z. B. M aus lauter verschiedenen Primfaktoren

$$p, p', p'', \ldots,$$

so ergiebt sich die gedachte Anzahl gleich

$$\prod_p (1 + p + p^2) = \prod_p \frac{p^3 - 1}{p - 1}.^{*)}$$

2. Der Ausgangspunkt der Eisenstein'schen Betrachtung ist nun der folgende: Transformirt man eine ternäre quadratische Form, z. B. die Form

$$\varphi = x^2 + x'^2 + x''^2$$

mittels einer Substitution, deren Modulus M ist, so geht sie bekanntlich in eine andere quadratische Form ψ über, deren Determinante gleich derjenigen der ersteren mal M^2 ist; wenn also $M = D^2$, so wird die Determinante von ψ gleich D^4 sein. Kann man aber die Substitution so wählen, dass die sämmtlichen Coefficienten von ψ durch D theilbar sind also

$$\psi = D \cdot f$$

gesetzt werden kann, wo f eine ganzzahlige ternäre Form, so wird diese letztere die Determinante D haben. Auf solche Weise lässt sich demnach durch eine ganzzahlige lineare Transformation aus der Form φ mit der Determinante 1 eine ternäre Form f mit beliebig vorgeschriebener Determinante D herleiten. Diese Betrachtung, welche in gleicher Weise auf quadratische Formen mit einer beliebigen ungeraden Anzahl $2n + 1$ von Unbestimmten übertragen werden kann, wenn man Substitutionen vom Modulus D^{n+1} verwendet, fordert zu der Aufgabe heraus, die sämmtlichen Substitutionen S zu ermitteln, welche das Gesagte leisten, nämlich die Form φ in das D-fache einer Form mit der Determinante D verwandeln. Der in voriger nr. gemachten Vorbemerkung zufolge kommt es nur darauf an, die nicht-äquivalenten oder auch die reducirten Substitutionen von der geforderten Beschaffenheit zu finden, und diese Aufgabe soll hier, jedoch unter Beschränkung auf solche Werthe von D, welche ungerade und ohne quadratischen Theiler sind, behandelt werden.

---

*) Vgl. zu dieser Nummer Cap. 3, nr. 10 des zweiten Abschnitts.

Sie fordert offenbar, die Elemente der Substitution (3) so zu bestimmen, dass die Congruenz

$$(\delta y)^2 + (\varepsilon' y + \delta' y')^2 + (\eta'' y + \theta'' y' + \delta'' y'')^2 \equiv 0 \pmod{D}$$

für alle Werthe von y, y', y'' erfüllt wird, d. h. dass sie den Congruenzen

$$\left.\begin{array}{lll} \delta^2 + \varepsilon'^2 + \eta''^2 \equiv 0, & \delta'^2 + \theta''^2 \equiv 0, & \delta''^2 \equiv 0 \\ \varepsilon'\delta' + \eta''\theta'' \equiv 0, & \eta''\delta'' \equiv 0, & \theta''\delta'' \equiv 0 \end{array}\right\} \pmod{D}$$

genügen. Die dritte derselben erheischt, dass δ'' theilbar ist durch D, wodurch dann die beiden letzten ebenfalls erfüllt werden, sodass nur noch den dreien:

$$(10) \qquad \delta^2 + \varepsilon'^2 + \eta''^2 \equiv 0, \quad \delta'^2 + \theta''^2 \equiv 0, \quad \varepsilon'\delta' + \eta''\theta'' \equiv 0$$

zu genügen bleibt. Die zweite der letzteren kann aber nur bestehen, wenn δ', θ'' durch jeden Primfaktor von D, welcher die Form $4h + 3$ hat, theilbar sind, und da $\delta\delta'\delta'' = D^2$ und δ'' schon durch D theilbar ist, so kann δ keinen jener Primfaktoren enthalten. Dagegen vertheilen sich die Primfaktoren von D, welche die Form $4h + 1$ haben, auf δ und δ' so, dass jeder, der nicht in δ' aufgeht, in δ enthalten und dass folglich $\delta'' = D$ ist; denn, ist p ein solcher Primfaktor, so folgt aus den Congruenzen (10)

$$\varepsilon'^2\delta'^2 \equiv \eta''^2\theta''^2 \equiv -\eta''^2\delta'^2 \pmod{p}$$

d. i.

$$\varepsilon'^2 + \eta''^2$$

und folglich auch δ^2 sowie δ selbst theilbar durch p.

Hieraus findet sich

$$\delta = P_1, \quad \delta' = P_2 Q, \quad \delta'' = D,$$

wenn man

$$D = P_1 P_2 \cdot Q$$

setzt, und unter Q das Produkt aller Primfaktoren von D von der Form $4h + 3$, unter $P_1 \cdot P_2$ irgend eine Zerlegung des Produktes P aller Primfaktoren von D von der Form $4h + 1$ in zwei Faktoren versteht. In Folge dieses Resultats lassen sich aber die Congruenzen (10), wenn man den Modulus in seine Faktoren auflöst, durch die andern ersetzen:

$$\left.\begin{aligned} \varepsilon'^2 + \eta''^2 &\equiv 0 \\ P_2^2 Q^2 + \theta''^2 &\equiv 0 \\ P_2 Q \varepsilon' + \eta''\theta'' &\equiv 0 \end{aligned}\right\} \pmod{P_1},$$

$$\left.\begin{aligned} P_1^2 + \varepsilon'^2 + \eta''^2 &\equiv 0 \\ \theta''^2 &\equiv 0 \\ \eta''\theta'' &\equiv 0 \end{aligned}\right\} \pmod{P_2 Q}.$$

Aus ihnen folgt zunächst

$$\theta'' = P_2 Q \cdot \lambda,$$

wo λ eine ganze Zahl ist, welche nicht-negativ und $< P_1$ anzunehmen ist, damit der vorgeschriebenen Bedingung

$$0 \overline{\gtrless} \theta'' < \delta''$$

genügt werde. Die beiden letzten Congruenzen (mod. P_1) gehen hierdurch in die anderen:

$$(11) \qquad 1 + \lambda^2 \equiv 0, \quad \varepsilon' + \eta''\lambda \equiv 0 \pmod{P_1}$$

über und zeigen, dass die erste jener Congruenzen eine Folge von ihnen ist, sodass man nur noch den eben geschriebenen Congruenzen, sowie der ersten der Congruenzen (mod. $P_2 Q$):

$$(12) \qquad P_1^2 + \varepsilon'^2 + \eta''^2 \equiv 0 \pmod{P_2 Q}$$

zu genügen hat. — Sei p_2 jeder Primfaktor von P_2 und $\tilde{\omega}_2$ ihre Anzahl, q jeder Primfaktor von Q: die Anzahl der (mod. δ') d. i. (mod. $P_2 Q$) incongruenten Systeme ε', η'', welche die letzte Congruenz erfüllen, ist dann

$$\Pi = \Pi(p_2 - 1) \cdot \Pi(q + 1)^{*)}.$$

Ist nun ε', η irgend eins dieser Systeme und λ irgend eine Wurzel der ersten der Congruenzen (11), so kann man eine Zahl η'' so wählen, dass $\eta'' \equiv \eta \pmod{P_2 Q}$ und zugleich auch $\varepsilon' + \eta''\lambda \equiv 0 \pmod{P_1}$ wird, sodass ε' und diese eindeutig (mod. $P_1 \cdot P_2 Q$) = (mod. δ'') definirte Zahl η'' die Congruenzen (11) und (12) erfüllen. Für jede Wurzel λ der ersten dieser Congruenzen — und deren Anzahl beträgt $2^{\tilde{\omega}_1}$, wenn P_1 aus $\tilde{\omega}_1$ Primfaktoren besteht — erhält man also Π, und somit im Ganzen

---

*) Dies folgt leicht aus den Formeln für die Anzahl Wurzeln quadratischer Congruenzen im siebenten Capitel des zweiten Abschnitts.

$$(13) \qquad 2^{\tilde{\omega}_1} \cdot \Pi = 2^{\tilde{\omega}_1} \cdot \Pi(p_2 - 1) \cdot \Pi(q + 1)$$

Systeme ε', η'', welche zugleich mit den Congruenzen (11) und (12) die Bedingungen (4) erfüllen. Ebenso gross ist demnach auch die Menge der reducirten Substitutionen, die wir suchen und welche der bestimmten Zerlegung

$$D = P_1 P_2 \cdot Q$$

entsprechen. Um ihre Gesammtmenge zu finden, sind die Ausdrücke (13), die allen möglichen solchen Zerlegungen von D zugehören, zu summiren. Nun kann man den Ausdruck (13), indem man $\tilde{\omega}_1 + \tilde{\omega}_2$, d. h. die Gesammtanzahl der verschiedenen Primfaktoren, aus denen $P = P_1 P_2$ besteht, mit $\tilde{\omega}$ bezeichnet, folgendermassen schreiben:

$$2^{\tilde{\omega}} \cdot \prod (q+1) \cdot \prod \left(\frac{p_2 - 1}{2}\right),$$

wo die zwei ersten Faktoren von der Zerlegung von P in zwei Faktoren unabhängig sind; die auf alle diese Zerlegungen bezügliche Summe der Ausdrücke ist also

$$2^{\tilde{\omega}} \cdot \prod (q+1) \cdot \sum \prod \left(\frac{p_2 - 1}{2}\right);$$

doch ist die Summe offenbar nichts anderes als das folgende Produkt, das auf sämmtliche Primfaktoren p von P erstreckt gedacht wird,

$$\prod \left(1 + \frac{p-1}{2}\right) = \prod \left(\frac{p+1}{2}\right);$$

mithin findet man endlich die Gesammtanzahl der verlangten reducirten Substitutionen gleich

$$\Pi(q+1) \cdot \Pi(p+1)$$

d. i. einfacher gleich

$$\Pi(d+1),$$

wenn man das Produkt auf *sämmtliche* Primfaktoren d von D erstreckt; sie ist also ebenso gross, wie die Summe aller Theiler von D.

3. Bei der soeben angestellten Betrachtung handelte es sich um die Transformationen vom Modulus D^2, welche φ in das D-fache einer ternären Form mit der Determinante D überhaupt verwandeln; verschieden davon ist die Aufgabe, diejenigen Transformationen der angegebenen Art zu er-

mitteln d. i. aus den gefundenen auszuscheiden, welche φ in das D-fache einer gegebenen ternären Form mit der Determinante D überführen. Man kann jedoch durch eine einfache Bemerkung die neue Aufgabe auf eine andere zurückführen, welche der bereits gelösten ganz analog ist. Seien

$$f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \quad \text{und} \quad F = \begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$$

die gegebene ternäre Form mit der Determinante D und ihre Adjungirte. Bezeichnet man mit S irgend eine Substitution, durch welche die Form φ in $D \cdot f$ übergeht, so folgt aus den Sätzen in nr. 4 des ersten Capitels, dass die Substitution Σ, welche durch Transposition von S entsteht und daher denselben Modulus D^2 hat wie S, die Form F überführt in $D^2 . \varphi$.

Jede solche Substitution Σ kann man aber gleich $\Sigma_0 \cdot T$ setzen, wo Σ_0 eine reducirte Substitution vom Modulus D^2 und T eine unimodulare Substitution ist; und, weil Σ die Form F in $D^2 \cdot \varphi$ verwandelt, und eine unimodulare Substitution T den gemeinsamen Faktor aller Coefficienten einer Form nicht verändert, muss die Form, in welche F durch Σ_0 übergeht, gleichfalls von der Gestalt $D^2 \cdot \psi$ und ψ mit φ äquivalent sein, nämlich durch die Substitution T in φ übergehen. Andererseits ergiebt sich aus der Beziehung zwischen den Determinanten der ursprünglichen und der transformirten Form, dass F durch eine Substitution vom Modulus D^2 nur in das D^2-fache einer solchen Form ψ verwandelt werden kann, welche mit φ äquivalent ist. Somit kann die Aufgabe, alle gedachten Substitutionen Σ zu finden, auf die andere zurückgeführt werden, sämmtliche reducirte Substitutionen Σ_0 vom Modulus D^2 zu ermitteln, welche F in das D^2-fache einer ternären Form überhaupt verwandeln. Hat man diese nämlich gefunden und ist T_0 eine Substitution, durch welche die der Substitution Σ_0 entsprechende Form ψ in φ übergeht, Θ aber jede Substitution, welche φ in sich selbst verwandelt, so haben die sämmtlichen Substitutionen Σ den Ausdruck

$$\Sigma_0 T_0 \Theta.$$

Hieraus entstehen aber endlich, wie leicht zu erkennen, die gesuchten Substitutionen S, wenn man

$$S = \vartheta \cdot S_0$$

setzt und unter S_0, ϑ die durch Transposition von $\Sigma_0 T_0$, Θ resp. hervorgehenden Substitutionen versteht, wo zu bemerken ist, dass dann ϑ ebenso wie Θ die sämmtlichen Substitutionen der Form φ in sich selbst bedeutet.

Bei dieser Untersuchung darf man nun (vgl. nr. 11 des zweiten Capitels) zur Vereinfachung voraussetzen, dass der dritte Coefficient A'' in F, sowie der erste Coefficient a in f, prim sei zu D, sodass die Aufgabe dann so gefasst werden kann: alle reducirten Substitutionen Σ_0 vom Modulus D^2 zu finden, welche, in $A'' \cdot F$ eingeführt, den Ausdruck theilbar machen durch D^2. Der algebraische Ausdruck dieses Umstandes ist das Stattfinden der Congruenz

$$(B'x + Bx' + A''x'')^2 + D \cdot (a'x^2 - 2b''xx' + ax'^2) \equiv 0 \pmod{D^2}$$

für

$$x = \delta y, \quad x' = \varepsilon' y + \delta' y', \quad x'' = \eta'' y + \theta'' y' + \delta'' y'',$$

eine Congruenz, welche offenbar dem Systeme der beiden andern:

$$B'x + Bx' + A''x'' \equiv 0, \quad a'x^2 - 2b''xx' + ax'^2 \equiv 0 \pmod{D}$$

äquivalent ist, und diese erfordern die folgenden sechs:

$$B'\delta + B\varepsilon' + A''\eta'' \equiv 0, \quad B\delta' + A''\theta'' \equiv 0, \quad A''\delta'' \equiv 0$$
$$a'\delta^2 - 2b''\delta\varepsilon' + a\varepsilon'^2 \equiv 0, \; -b''\delta\delta' + a\varepsilon'\delta' \equiv 0, \; a\delta'^2 \equiv 0.$$

Aus ihnen folgt zunächst nach der über a, A'' gemachten Annahme, dass δ', δ'' theilbar sind durch D oder vielmehr wegen der Gleichung

$$\delta\delta'\delta'' = D^2,$$

dass

$$\delta' = \delta'' = D \quad \text{und} \quad \delta = 1$$

sind. In Folge davon ist die vorletzte Congruenz von selbst erfüllt, die zweite ergiebt — mit Rücksicht auf die vorgeschriebene Bedingung (4) —

$$\theta'' = 0,$$

und die noch übrigen nehmen die Form an:

$$(14) \quad B' + B\varepsilon' + A''\eta'' \equiv 0, \quad a' - 2b''\varepsilon' + a\varepsilon'^2 \equiv 0,$$

deren letzte auch so gestaltet werden kann:

(14a) $(a\varepsilon' - b'')^2 \equiv b''^2 - aa' \equiv - A''$ (mod. D).

Hieraus ersieht man, dass es Substitutionen der verlangten Beschaffenheit nur giebt, wenn $-A''$ quadratischer Rest von D ist, d. h. wenn die Form f einem durch diese Bedingung (da $\Omega = 1$ ist) vollständig bestimmten Geschlechte G von Formen angehörig ist. Setzt man also f als eine Form dieses Geschlechtes voraus, so hat die Congruenz (14a) $2^\varkappa$ verschiedene Wurzeln, wenn $\varkappa$ die Anzahl der Primfaktoren bezeichnet, aus denen D sich zusammensetzt, und zu jeder dieser Wurzeln gehört eine bestimmte Zahl $\varepsilon' < D$ d. h. $< \delta'$, welche die Congruenz erfüllt, und sodann auch nur eine bestimmte Zahl $\eta'' < D$ d. i. $< \delta''$, für welche die andere der Congruenzen (14) erfüllt ist. Somit giebt es $2^\varkappa$ Systeme ε', η'' d. i. $2^\varkappa$ reducirte Substitutionen

$$\Sigma_0 = \begin{pmatrix} 1, & 0, & 0 \\ \varepsilon', & D, & 0 \\ \eta'', & 0, & D \end{pmatrix},$$

wie sie gesucht werden.

Ebenso viel Substitutionen S_0 sind aber vorhanden, und da die Anzahl der Substitutionen ϑ, welche φ in sich selbst verwandeln, nach nr. 3 des vierten Capitels gleich 24 ist, so ist $24 \cdot 2^\varkappa$ die Anzahl der Substitutionen S, um die es sich hier handelt: Für jede Form f des Geschlechts G giebt es $24 \cdot 2^\varkappa$ Substitutionen, durch welche φ in $D \cdot f$ verwandelt wird.

Ist aber S eine solche Substitution, so ist ersichtlich jede Substitution $S \cdot T$ auch eine solche, wenn T jede der Substitutionen bezeichnet, durch welche f in sich selbst übergeht und deren Anzahl θ heissen mag; diese sind sämmtlich äquivalent; aber auch umgekehrt ergiebt die Formel $S \cdot T$ offenbar alle mit S äquivalenten unter den $24 \cdot 2^\varkappa$ Substitutionen, wenn man für T jene θ Substitutionen einsetzt, und somit vertheilen sich die $24 \cdot 2^\varkappa$ Substitutionen auf $\frac{24 \cdot 2^\varkappa}{\theta}$ Classen äquivalenter Substitutionen der gedachten Art, oder:

es giebt $\frac{24 \cdot 2^{\varkappa}}{\theta}$ nicht-äquivalente Substitutionen, durch welche φ übergeht in $D \cdot f$.

4. Da jede Substitution vom Modulus D^2 durch Zusammensetzung mit einer bestimmten unimodularen Substitution T in eine reducirte Substitution vom Modulus D^2 übergeht, die Substitution T aber die Form f in eine äquivalente verwandelt, kann man dies Resultat auch so aussprechen: es giebt $\frac{24 \cdot 2^{\varkappa}}{\theta}$ reducirte Substitutionen vom Modulus D^2, welche φ in das D-fache einer Form der Classe verwandeln, der f angehört. Den so gewonnenen Satz verbinden wir nun mit demjenigen der nr. 2. Denkt man sich die verschiedenen Classen $C, C', C'', \ldots$ des Geschlechts G und bezeichnet mit $\theta, \theta', \theta'', \ldots$ die diesen Classen zugehörigen Transformationszahlen d. h. die Anzahl der Substitutionen, durch welche resp. jede ihrer Formen in sich selbst übergeht, so giebt es beziehungsweise

$$(15) \qquad \frac{24 \cdot 2^{\varkappa}}{\theta}, \quad \frac{24 \cdot 2^{\varkappa}}{\theta'}, \quad \frac{24 \cdot 2^{\varkappa}}{\theta''}, \ldots$$

reducirte Substitutionen vom Modulus D^2, welche φ in das D-fache einer Form jener Classen verwandeln. Da aber die Anzahl solcher Substitutionen, welche φ überhaupt in das D-fache einer ternären Form mit der Determinante D verwandeln, gleich $\Pi(d+1)$ ist, und die ternäre Form dann nur dem Geschlechte G angehören kann, muss die Summe der Zahlen (15) dieser Zahl $\Pi(d+1)$ gleich, oder

$$\frac{1}{\theta} + \frac{1}{\theta'} + \frac{1}{\theta''} + \cdots$$

d. i. das Maass des Geschlechts G gleich

$$(16) \qquad \frac{1}{24 \cdot 2^{\varkappa}} \cdot \prod (d+1)$$

sein. Dies ist die Formel, welche Eisenstein an der angegebenen Stelle der Berl. Monatsberichte abgeleitet hat; sie ist als besonders einfacher Fall in einer anderen enthalten, die von ihm ohne Beweis im 35. Band des Crelle'schen Journals mitgetheilt worden ist und durch eine Verallgemeinerung der voraufgehenden Untersuchung gewonnen werden kann. Zur

Herleitung der letzteren bedienen wir uns aber nunmehr nach dem Vorgange von Smith und Minkowski*) allgemeinerer Principien, nämlich der analytischen Methoden von Dirichlet.

5. Betrachtet man zu diesem Zwecke ein gegebenes Geschlecht ternärer Formen der Ordnung (Ω, Δ) und bezeichnet mit

(17) $$f, f', f'', \dots$$

irgend welche Repräsentanten der Classen, welche es bilden, sowie mit

(18) $$\mathfrak{F}, \mathfrak{F}', \mathfrak{F}'', \dots$$

ihre bezüglichen Reciproken. Man verstehe weiter unter M'' jede positive zu $2\Omega\Delta$ prime Zahl, welche der Bedingung

$$\Omega M'' \equiv 1 \pmod{4}$$

Genüge leistet. Soll eine Zahl dieser Art durch eine der Formen (18), etwa durch $\mathfrak{F}$, darstellbar sein, so muss sie die quadratischen Charaktere des Geschlechts aufweisen, d. h. es muss

$$\left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right), \quad \left(\frac{M''}{\delta'}\right) = \left(\frac{\mathfrak{F}}{\delta'}\right), \dots$$

sein, wenn wieder $\delta, \delta', \delta'', \dots$ die verschiedenen Primfaktoren von Δ bedeuten. Umgekehrt folgt aber aus nr. 6 des fünften Capitels, dass jede der Zahlen M'', welcher diese quadratischen Charaktere eignen, durch die Reciproke einer der Formen des Geschlechts also durch eine der Formen (18) darstellbar ist. Indem man nun die Gesammtheit aller so bestimmten Zahlen M'' oder vielmehr die ihrer Darstellungen durch das System der Formen (18) ins Auge fasst, wird eine doppelte Abzählung ihrer Maasse zu einer Gleichung führen, aus welcher das Maass des Geschlechts sich unmittelbar ausdrücken lässt.

Offenbar werden alle jene Darstellungen erhalten, wenn in den sämmtlichen Formen (18) die ganzzahligen Unbestimmten x, x', x'' auf alle Weise so gewählt werden, dass die Werthe der Formen, welche, da es sich um positive Formen

*) S. die im zweiten Capitel angeführten Abhandlungen der genannten beiden Mathematiker.

handelt, von selbst positiv sein werden, auch prim zu $2\Omega\Delta$ werden und für $\mathfrak{F}$ der Congruenz $\Omega \cdot \mathfrak{F} \equiv 1 \pmod{4}$, für die anderen Formen den analogen Congruenzen genügen. Bezeichnet man durch $\theta(\mathfrak{F})$ die Anzahl der Transformationen von $\mathfrak{F}$ in sich selbst, so ist $\theta(\mathfrak{F})^{-1}$ das Maass jeder Darstellung, welche durch die Form $\mathfrak{F}$ geschieht. Dieses Maass soll mit

$$\frac{1}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}}$$

multiplicirt werden, wo ϱ eine positive Veränderliche bedeute, das so definirte Produkt für die Gesammtheit der zuvor angegebenen Systeme x, x', x'' und damit die folgende Summe gebildet werden:

$$\sum_{\mathfrak{F}}\left(\sum \frac{\theta(\mathfrak{F})^{-1}}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}}\right),$$

wo die äussere Summation sich auf alle Formen (18), die innere aber auf alle ganzzahligen x, x', x'' bezieht, für welche die jedesmalige Form $\mathfrak{F}$ prim zu $2\Omega\Delta$ und

$$\Omega \cdot \mathfrak{F} \equiv 1 \pmod{4}$$

wird. Diese Summe ist für ein positives ϱ absolut convergent, also von der Reihenfolge ihrer Glieder unabhängig. Denkt man daher diejenigen ihrer Glieder zusammengefasst, in denen $\mathfrak{F}(x, x', x'')$ die gleiche der oben definirten Zahlen M'' darstellt, so erhält man offenbar für jede dieser Zahlen M'' den Bruch $\frac{1}{M''^{3/2(1+\varrho)}}$ multiplicirt in die Summe der Maasse ihrer einzelnen Darstellungen durch die Formen (18) d. i. multiplicirt in „das Maass“ ihrer Darstellungen durch dieselben. Nennt man letzteres einfach (M''), so wird hiernach die vorige Summe, passend geordnet, auch folgendermassen geschrieben werden können:

$$\sum \frac{(M'')}{M''^{3/2(1+\varrho)}},$$

und man gewinnt nachstehende, für die fernere Betrachtung grundlegende Beziehung:

$$\text{(19)} \qquad \sum_{\mathfrak{F}}\left(\sum \frac{\theta(\mathfrak{F})^{-1}}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}}\right) = \sum \frac{(M'')}{M''^{3/2(1+\varrho)}},$$

in welcher die Summation rechts über alle oben definirten Zahlen M'' erstreckt werden muss.

6. Man beginne dagegen nun die Ausführung der doppelten Summation mit der auf eine bestimmte Form $\mathfrak{F}$ bezüglichen Summe, bei welcher der für alle Glieder gemeinsame Zähler vor das Summenzeichen gesetzt werden kann, sodass zu bestimmen bleibt

$$(20) \qquad \sum \frac{1}{\mathfrak{F}(x, x', x'')^{1/2(1+\varrho)}}.$$

Ueberblicken wir vor allem das Gebiet der zulässigen Werthsysteme x, x', x''. Wählt man in dem Smith'schen Satze in nr. 7 des zweiten Capitels $N = 4\Omega\Delta$ und vertauscht, was erlaubt ist, wenn man gleichzeitig Ω und Δ mit einander vertauscht, die reciproken Formen, so darf man für die in ihren Classen beliebig zu nehmenden Repräsentanten f und $\mathfrak{F}$ folgende Congruenzen ansetzen:

$$(21) \qquad \begin{cases} \mathfrak{F} \equiv \alpha x^2 + \beta\Delta x'^2 + \gamma\Omega\Delta x''^2 \\ f \equiv \beta\gamma\Omega\Delta x^2 + \gamma\alpha\Omega x'^2 + \alpha\beta x''^2 \end{cases} \pmod{4\Omega\Delta},$$

während

$$\alpha\beta\gamma \equiv 1 \pmod{4\Omega\Delta} \text{ und } \alpha\Omega \equiv 1 \pmod{4}$$

ist. Man nenne nun wieder r die Primfaktoren, welche Ω, Δ gemeinsam sind, δ diejenigen, die nur in Δ, ω diejenigen, die nur in Ω aufgehen, und setze

$$(22) \qquad \Pi = 4\Pi(r) \cdot \Pi(\delta) \cdot \Pi(\omega).$$

Aus der Congruenz (21) folgt dann zunächst, dass, damit $\mathfrak{F}$ durch r nicht theilbar werde, x prim zu r gewählt werden muss, während x', x'' beliebig bleiben, es giebt also

$$(r-1) \cdot r^2 \pmod{r}$$

incongruente zulässige Werthsysteme x, x', x''; aus gleicher Erwägung giebt es

$$(\delta - 1) \cdot \delta^2 \pmod{\delta}$$

incongruente zulässige Werthsysteme. Damit aber $\mathfrak{F}$ durch ω nicht theilbar werde, darf es $\alpha x^2 + \beta\Delta x'^2$ nicht sein; giebt man nun x' einen durch ω theilbaren Werth, so muss x nicht theilbar durch ω gewählt werden, was $\omega - 1$ Systeme x, x' liefert; für einen durch ω nicht theilbaren Werth x' dagegen

darf man x jeden Werth beilegen, falls $-\alpha\beta\Delta$ oder, was wegen der zweiten der Congruenzen (21) hierfür gesetzt werden darf, $-\Delta\cdot f$ quadratischer Nichtrest (mod. ω) ist, dagegen nur $\omega - 2$ (mod. ω) incongruente Werthe im entgegengesetzten Falle. So findet man, da x'' beliebig bleibt,

$$\omega\cdot\left[1\cdot(\omega-1)+(\omega-1)\left(\omega-1-\left(\frac{-\Delta f}{\omega}\right)\right)\right]$$
$$=\omega(\omega-1)\left(\omega-\left(\frac{-\Delta f}{\omega}\right)\right)$$

(mod. ω) incongruente zulässige Werthsysteme x, x', x''. Endlich nimmt die Bedingung $\Omega\mathfrak{J}\equiv 1$ (mod. 4) die Gestalt an:

$$x^2+(\beta\Omega x'^2+\gamma x''^2)\Delta\equiv 1 \text{ (mod. 4)},$$

während aus den Congruenzen

$$\alpha\beta\gamma\equiv 1 \quad \text{und } \alpha\Omega\equiv 1 \text{ (mod. 4)}$$

sich

$$\beta\Omega\equiv\gamma \text{ (mod. 4)}$$

ergiebt. Ertheilt man nun zuerst x einen geraden Werth, so muss

$$\beta\Omega x'^2+\gamma x''^2\equiv\Delta \text{ (mod. 4)}$$

werden, was, wie man leicht einsieht,

$$4\left(1+(-1)^{\frac{\Delta-1}{2}+\frac{\beta\Omega-1}{2}}\right)$$

Lösungen x, x', x'' verstattet; für ein ungerades x aber muss

$$\beta\Omega x'^2+\gamma x''^2\equiv 0 \text{ (mod. 4)}$$

werden, was mit $x'^2+x''^2\equiv 0$ gleichbedeutend ist, also 4 Lösungen gestattet. Somit findet man im Ganzen

$$8\left(2+(-1)^{\frac{\Delta-1}{2}+\frac{\beta\Omega-1}{2}}\right)$$

Lösungen x, x', x''. Führt man aber die durch die Formel (40) des zweiten Capitels definirte Einheit E ein, so findet sich diese hier gleich

$$E=(-1)^{\frac{\alpha\Omega+1}{2}\cdot\frac{\alpha\beta\Delta+1}{2}}$$

d. i. nach einfachen Umformungen mit Rücksicht auf die Congruenz $\alpha\Omega\equiv 1$ (mod. 4):

$$E=(-1)^{\frac{\Delta-1}{2}+\frac{\beta\Omega-1}{2}+1}.$$

Demnach ist die Anzahl der (mod. 4) incongruenten zulässigen Systeme x, x', x'' gleich

$$8(2 - E).$$

Durch Combination der nach den einzelnen Moduln 4, r, δ, ω zulässigen Werthsysteme x, x', x'' findet man nun sogleich die Anzahl der zulässigen, nach dem (mod. Π) incongruenten Systeme gleich

$$(23)\qquad \begin{cases} 8(2 - E) \cdot \Pi r^2(r - 1) \cdot \Pi \delta^2(\delta - 1) \\ \qquad \cdot \Pi \omega(\omega - 1)\left(\omega - \left(\frac{-\Delta f}{\omega}\right)\right), \end{cases}$$

wo die einzelnen Multiplikationen auf die sämmtlichen Primfaktoren der bezeichneten Categorieen bezogen werden müssen.

Nennt man $\mathfrak{x}, \mathfrak{x}', \mathfrak{x}''$ jedes dieser Systeme, so erhält man sämmtliche in der Summe (20) zu berücksichtigenden Werthsysteme x, x', x'' durch die Formeln

$$(24)\qquad x = \Pi \cdot y + \mathfrak{x}, \quad x' = \Pi \cdot y' + \mathfrak{x}', \quad x'' = \Pi \cdot y'' + \mathfrak{x}'',$$

wenn man in ihnen y, y', y'' für jedes System $\mathfrak{x}, \mathfrak{x}', \mathfrak{x}''$ sämmtliche ganzzahligen Werthe durchlaufen lässt. Es soll nun zunächst derjenige Bestandtheil der Summe untersucht werden, welcher einem einzigen der Systeme $\mathfrak{x}, \mathfrak{x}', \mathfrak{x}''$ entspricht.

Betrachtet man in dieser Partialsumme zunächst nur diejenigen x, x', x'' von der Form (24), für welche der Werth der Form $\mathfrak{F}$ den Werth $t^{2/3}$ nicht überschreitet, und nennt T die Anzahl dieser Systeme, so hat nach dem Dirichlet'schen Reihensatze, auf welchen seine analytischen Methoden wesentlich begründet sind*), die Partialsumme

$$\varrho \cdot \sum{}' \frac{1}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}}$$

bei einem positiv gegen Null convergirenden ϱ denselben Grenzwerth, gegen welchen bei unendlich wachsendem t der Quotient $\frac{T}{t}$ convergirt:

$$(25)\qquad \lim_{\varrho=0} \varrho \sum{}' \frac{1}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}} = \lim_{t=\infty} \frac{T}{t}.$$

---

*) S. Analyt. Zahlentheorie S. 67.

Andererseits ist, wenn man

$$z = \frac{x}{t^{1/3}}, \quad z' = \frac{x'}{t^{1/3}}, \quad z'' = \frac{x''}{t^{1/3}}$$

setzt und z, z', z'' als rechtwinklige Coordinaten eines Punktes betrachtet, T die Anzahl der Netzpunkte

$$z = \frac{\Pi}{t^{1/3}} \cdot y + \frac{\xi}{t^{1/3}}, \quad z' = \frac{\Pi}{t^{1/3}} \cdot y' + \frac{\xi'}{t^{1/3}}, \quad z'' = \frac{\Pi}{t^{1/3}} \cdot y'' + \frac{\xi''}{t^{1/3}},$$

welche in das Innere des durch die Ungleichheit

$$\mathfrak{F}(z, z', z'') \overline{\gtrless} 1$$

definirten ellipsoidischen Raumes fallen, und folglich ist nach einem allgemeinen Satze*)

$$\Pi^3 \cdot \lim_{t=\infty} \frac{T}{t}$$

dem über jenen Raum erstreckten dreifachen Integrale

$$\int dz \, dz' \, dz''$$

d. i. dem Inhalte des Ellipsoides gleich, der bekanntlich durch den Ausdruck

$$\frac{4}{3} \cdot \frac{\pi}{\sqrt{\Delta^2 \Omega}}$$

gemessen wird. Also nimmt die Formel (25) die Gestalt an:

$$(26) \qquad \lim_{\varrho=0} \varrho \sum{}' \frac{1}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}} = \frac{4}{3} \cdot \frac{\pi}{\sqrt{\Delta^2 \Omega}} \cdot \frac{1}{\Pi^3}.$$

Da der gefundene Werth unabhängig ist von dem besonderen Systeme ξ, ξ', ξ'', auf welches die Partialsumme sich bezog, so findet sich nun ohne Weiteres für die Gesammtsumme (20) die Bestimmung:

$$(27) \qquad \lim_{\varrho=0} \varrho \sum \frac{1}{\mathfrak{F}(x, x', x'')^{3/2(1+\varrho)}} = \frac{4}{3} \cdot \frac{\pi}{\Delta \Omega^{1/2}} \cdot \frac{\mathsf{A}}{\Pi^3},$$

wo A zur Abkürzung steht für den Ausdruck (23). Dieser Werth zeigt sich nun aber wieder ganz unabhängig von der besonderen Form $\mathfrak{F}$, auf welche die Summe sich bezieht. Wird demnach die Gleichung (19) beiderseits mit ϱ multiplicirt, so findet sich bei unendlicher Abnahme

*) S. Analyt. Zahlentheorie S. 437.

von ϱ für den Grenzwerth ihrer *linken* Seite der Ausdruck:

$$\frac{4}{3}\cdot\frac{\pi}{\Omega^{1/2}\Delta}\cdot\frac{\mathsf{A}}{\Pi^3}\cdot\sum_{\mathfrak{F}}\frac{1}{\theta(\mathfrak{F})}$$

d. i.

$$\frac{4}{3}\cdot\frac{\pi\mathsf{A}}{\Omega^{1/2}\Delta}\cdot\frac{\mathsf{M}}{\Pi^3},\tag{28}$$

wenn unter M das Maass des betrachteten Geschlechts ternärer Formen verstanden wird.

7. Es handelt sich nun weiter um die Ermittlung des Grenzwerthes der mit ϱ multiplicirten rechten Seite der Gleichung (19):

$$\varrho\cdot\sum\frac{(M'')}{M''^{3/2(1+\varrho)}}\tag{29}$$

für $\varrho = 0$. Hier erinnere man sich vor allem des Satzes in nr. 3 des sechsten Capitels. Handelte es sich nur um eigentliche Darstellungen der Zahlen M'' durch die Formen (18), so würde statt (M'') der Ausdruck $2^\mu\cdot\frac{g}{\tau}$ zu setzen sein, wo μ die Anzahl der Primfaktoren von M'' und g die Anzahl der Classen eines gewissen Geschlechts positiver eigentlich primitiver binärer Formen mit der Determinante $-\Omega M''$ ist, eine Anzahl, für welche die Anzahl der Classen des Hauptgeschlechts oder, wenn $H(-\Omega M'')$ die Anzahl aller eigentlich primitiven Formen jener Determinante, λ die Anzahl der Primfaktoren von Ω, also $2^{\mu+\lambda}$ die Anzahl der Geschlechter für die Determinante $-\Omega M''\equiv 3 \pmod 4$ bezeichnet, der Ausdruck

$$\frac{H(-\Omega M'')}{2^{\mu+\lambda}}$$

gesetzt werden kann. Das Maass der eigentlichen Darstellungen durch die Formen (18) ist also

$$\frac{1}{2^\lambda}\cdot\frac{H(-\Omega M'')}{\tau}.$$

Nun entspricht jeder uneigentlichen Darstellung von M'' durch eine Form $\mathfrak{F}$, bei welcher die darstellenden Zahlen den grössten gemeinsamen Theiler d haben, eine eigentliche Darstellung von $\frac{M''}{d^2}$ durch diese Form und umgekehrt, und das

Maass beider Darstellungen ist dasselbe; die Zahl $\frac{M''}{d^2}$ gehört aber ebenfalls zur Categorie der Zahlen, welche wir M'' genannt haben. Hiernach wird offenbar das Maass solcher uneigentlichen Darstellungen von M'' durch die Formen (18) gleich

$$\frac{1}{2^\lambda} \cdot \frac{H\left(-\frac{\Omega M''}{d^2}\right)}{\tau_d},$$

wenn τ_d die Anzahl der Transformationen einer binären Form der Determinante $\frac{-\Omega M''}{d^2}$ in sich selbst bezeichnet; dieser Ausdruck enthält den vorigen als den besonderen, $d = 1$ entsprechenden Fall und τ ist identisch mit τ_1. Demnach wird schliesslich

$$(30) \qquad (M'') = \frac{1}{2^\lambda} \cdot \sum_{d^2} \frac{H\left(-\frac{\Omega M''}{d^2}\right)}{\tau_d}$$

sein, wenn die Summation sich auf sämmtliche quadratische Theiler d^2 von M'' erstreckt.

Nachdem so ein Ausdruck für (M'') ermittelt worden, bemerke man weiter, dass die sämmtlichen Zahlen M'' in einer Anzahl arithmetischer Reihen enthalten sind von der Form

$$4\Omega\Delta z + m_1, \quad 4\Omega\Delta z + m_2, \quad \cdots 4\Omega\Delta z + m_\varkappa,$$

wo

$$0 < m_1 < m_2 \cdots < m_\varkappa < 4\Omega\Delta$$

ist; zwei, der Grösse nach aufeinanderfolgende dieser Zahlen, M und M_1, werden also eins der beiden Verhältnisse

$$\frac{4\Omega\Delta z + m_i}{4\Omega\Delta z + m_{i+1}}, \quad \frac{4\Omega\Delta z + m_\varkappa}{4\Omega\Delta z + 4\Omega\Delta + m_1}$$

zu einander haben und demnach wird bei unendlich wachsenden M, M_1

$$\lim. \frac{M}{M_1} = 1$$

sein. Hiernach schliesst man aus einem allgemeinen, von den Dirichlet'schen Reihen geltenden Satze*), dass, wenn

*) S. analytische Zahlentheorie S. 66.

(31) $$\frac{\Sigma(M'')}{M^{3/2}},$$

wo die Summe sich über alle Zahlen M'' der gedachten Categorie bis zur bestimmten Zahl M derselben hin erstreckt, bei unendlich wachsendem M gegen einen Grenzwerth L convergirt, folgende Gleichung besteht:

(32) $$\lim_{\varrho=0} \varrho \sum \frac{(M'')}{M''^{3/2(1+\varrho)}} = L.$$

Es wird also darauf ankommen, den Ausdruck (31) in dieser Hinsicht näher zu untersuchen.

Nun ist

$$\frac{H\left(-\frac{\Omega M''}{d^2}\right)}{\tau_d}$$

das Maass aller nicht äquivalenten positiven und eigentlich-primitiven binären Formen mit der Determinante $-\frac{\Omega M''}{d^2}$ oder auch aller nicht äquivalenten abgeleiteten Formen mit der Determinante $-\Omega M''$, deren Coefficienten x, y, z den grössten gemeinsamen Theiler d haben. Die Summe, welche in der Formel (30) auftritt, ist also das Maass aller nicht äquivalenten primitiven und nicht primitiven Formen (x, y, z), deren Determinante $-\Omega M''$ ist und deren Coefficienten keinen gemeinsamen Theiler mit Ω haben. Um aber die nicht äquivalenten Formen (x, y, z) dieser Art zu umfassen, sind, der Lehre von den reducirten binären Formen gemäss, ihre Coefficienten den Beschränkungen zu unterwerfen, dass

(33) $$x > 0, \quad \eta > 0, \quad z > 0, \quad 2\eta < x < z$$

sind, wo η den numerischen Werth von y bedeutet. Aus diesen Ungleichheiten folgt

(34) $$\eta < \sqrt{\tfrac{1}{3}\Omega M''}.$$

Es ist zulässig, dass eine der Gleichheiten

(35) $$\eta = 0, \quad 2\eta = x, \quad x = z$$

oder auch gleichzeitig die erste und letzte derselben stattfindet. — Jedem zulässigen Werthsysteme x, η, z, für welches keine dieser Gleichheiten stattfindet, gehören zwei nicht äqui-

valente Formen (x, η, z) und $(x, -\eta, z)$ zu, für welche die Determinante $-\Omega M''$ wegen (34) nicht -1 sein kann, deren Maass also gleich $\frac{1}{2}$ ist; die Summe der Maasse dieser Formen ist also 1. Findet eine jener Gleichheiten statt, so entspricht dem Werthsysteme x, η, z nur eine Classe, welche durch die Form (x, η, z) repräsentirt wird und für welche das Maass gleich $\frac{1}{2}$ gefunden wird. Die beiden Gleichheiten

$$\eta = 0, \quad x = z$$

aber können nur stattfinden, wenn $\Omega = 1$ und M'' eine Quadratzahl ist, und in diesem Falle wäre die entsprechende Form $(x, 0, x)$ abgeleitet aus der Form $(1, 0, 1)$ und folglich ihr Maass gleich $\frac{1}{4}$. Versteht man demnach unter x, η, z jedes ganzzahlige Werthsystem ohne gemeinsamen Theiler mit Ω, für welches

$$xz - \eta^2 = \Omega M'' \tag{36}$$

ist und die Ungleichheiten (33) resp. die Gleichheiten (35), soweit diese zulässig sind, erfüllt werden, und unter dem Symbole

$$[xz - \eta^2]_{\Omega M''}$$

den Werth $1, \frac{1}{2}$ oder $\frac{1}{4}$, jenachdem x, η, z resp. keine, eine oder die beiden zulässigen der Gleichheiten (35) erfüllen, so leuchtet aus dem Vorbemerkten ein, dass die in (30) auftretende Summe der über alle diese ganzzahligen Systeme x, η, z erstreckten Summe

$$\sum [xz - \eta^2]_{\Omega M''}$$

gleich und folglich

$$(M'') = \frac{1}{2^\lambda} \cdot \sum [xz - \eta^2]_{\Omega M}$$

also

$$\frac{\Sigma(M'')}{M^{3/2}} = \frac{1}{2^\lambda M^{3/2}} \cdot \sum_{M''} \left(\sum [xz - \eta^2]_{\Omega M''} \right) \tag{37}$$

sein muss, wo die äussere der beiden Summationen sich über alle solche Zahlen M'' erstreckt, welche $\overline{\gtrless} M$ sind.

8. Es gilt nun, die Gesammtheit der bei dieser Doppelsumme in Frage kommenden Werthsysteme x, η, z zu überschauen. Nach (36) soll die Zahl $\frac{xz - \eta^2}{\Omega}$ eine Zahl M'' werden; aus diesem Umstande fliessen folgende Forderungen:

erstens muss

$$xz - \eta^2 \equiv 1 \pmod{4}$$

sein;

zweitens muss $xz - \eta^2$ durch Ω, also durch jeden der Primfaktoren ω, oder genauer, wenn ω^i die höchste Potenz desselben bedeutet, welche in ω aufgeht, durch ω^i aber, weil M'' prim ist zu Ω, nicht durch ω^{i+1} aufgehen, auch dürfen x, η, z nicht gleichzeitig durch ω theilbar sein;

drittens muss $\frac{xz - \eta^2}{\Omega}$ in Bezug auf jeden Primfaktor δ von Δ einen vorgeschriebenen quadratischen Charakter, nämlich den Charakter $\left(\frac{\mathfrak{F}}{\delta}\right)$ haben.

Für die Primfaktoren, welche mit r bezeichnet wurden, muss, weil sie in Ω und Δ aufgehen, sowohl der zweite als der dritte dieser Punkte erfüllt sein.

Erstens. Damit $xz - \eta^2 \equiv 1 \pmod{4}$ sei, darf man entweder $\eta \equiv 0, 2 \pmod{4}$ und dann

$$x \equiv z \equiv 1 \quad \text{oder} \quad x \equiv z \equiv 3$$

wählen, oder $\eta \equiv 1, 3$ und dann

$$x \equiv 2,\ z \equiv 1, 3 \quad \text{oder} \quad z \equiv 2,\ x \equiv 1, 3,$$

was im Ganzen zwölf (mod. 4) zulässige Restsysteme x, η, z giebt.

Zweitens. Sei m eine gegebene Zahl, p eine ungerade Primzahl und A die Anzahl derjenigen, nicht durch p theilbaren Restsysteme x, η, z (mod. p^i), für welche

$$xz \equiv \eta^2 \pmod{p^i}$$

ist. Setzt man alsdann

$$x' = up^i + x, \quad \eta' = vp^i + \eta, \quad z' = wp^i + z,$$

so folgt

$$x'z' - \eta'^2 \equiv (xw + zu - 2v\eta)p^i + xz - \eta^2 \pmod{p^{i+1}}$$

also

$$\frac{x'z' - \eta'^2}{p^i} \equiv xw + zu - 2\eta v + \frac{xz - \eta^2}{p^i} \pmod{p}.$$

Da wenigstens eine der Zahlen x, η, z nicht theilbar ist durch p, kann man der Congruenz

$$(38) \qquad \frac{x'z' - \eta'^2}{p^i} \equiv m \pmod{p}$$

stets auf eindeutige Weise genügen, nachdem man zwei der Zahlen u, v, w beliebig gewählt hat, was für jedes der A Restsysteme x, z, η demnach p^2 nach dem Modulus p^{i+1} incongruente und nicht gleichzeitig durch p theilbare Restsysteme x', η', z' giebt, welche der Congruenz (38) genügen. Diese Congruenz hat also $A \cdot p^2 \pmod{p^{i+1}}$ incongruente Lösungen.

Nun hat die Congruenz

$$xz - \eta^2 \equiv 0 \pmod{p},$$

wie man sich leicht überzeugt, $p^2 - 1 \pmod{p}$ incongruente, nicht durch p aufgehende Lösungen. Wählt man daher $m = 0$, $i = 1$, so ergeben sich dem eben Bewiesenen zufolge

$$(p^2 - 1)p^2 \pmod{p^2}$$

incongruente Lösungen der bezeichneten Art für die Congruenz

$$xz - \eta^2 \equiv 0 \pmod{p^2}$$

und allgemeiner $(p^2 - 1) \cdot p^{2(i-1)}$ für die Congruenz

$$xz - \eta^2 \equiv 0 \pmod{p^i},$$

sodass für jedes m die Anzahl der $\pmod{p^{i+1}}$ incongruenten Lösungen gleicher Art für die Congruenz

$$xz - \eta^2 \equiv m \cdot p^i \pmod{p^{i+1}}$$

gleich $(p^2 - 1) \cdot p^{2i}$ wird.

Ist nun p eine der mit ω bezeichneten Primzahlen, die nicht auch in Δ aufgehen, so darf man unter m jeden nicht durch ω aufgehenden Rest $\pmod{\omega}$ verstehen. Demnach wird die Anzahl der $\pmod{\omega^{i+1}}$ zulässigen Restsysteme x, η, z alsdann gleich

$$(\omega^2 - 1)(\omega - 1)\omega^{2i}$$

sein. — Ist dagegen p einer der Primfaktoren r, so muss $\frac{xz - \eta^2}{\Omega}$ also auch $\frac{xz - \eta^2}{r^i}$ einen vorgeschriebenen quadratischen Charakter $\pmod{r}$ haben; in diesem Falle darf daher m nur als einer derjenigen $\frac{r-1}{2}$ Reste $\pmod{r}$ gewählt werden, denen

dieser Charakter zukommt, und demnach giebt es nur

$$\frac{1}{2}(r^2-1)(r-1)r^{2i}$$

(mod. r^{i+1}) zulässige Restsysteme x, η, z.

Drittens, damit $\frac{xz-\eta^2}{\Omega}$ in Bezug auf einen der mit δ bezeichneten Primfaktoren von Δ den vorgeschriebenen quadratischen Charakter $\left(\frac{\mathfrak{F}}{\delta}\right)$ erhält, muss $xz-\eta^2$ selbst den Charakter $\left(\frac{\Omega\mathfrak{F}}{\delta}\right)$ erhalten. Ist demnach m irgend einer der $\frac{\delta-1}{2}$ Reste (mod. δ), welchen dieser Charakter zukommt, so muss

$$xz-\eta^2 \equiv m \pmod{\delta}$$

sein. Hier darf $\eta\equiv 0$ und dann $xz\equiv m$ gesetzt werden, was $\delta-1$ Systeme x, η, z giebt; wird aber $\eta\equiv 1, 2, \cdots \delta-1$ gesetzt und ist zuerst $\left(\frac{-m}{\delta}\right)=-1$, so wird für keinen dieser Werthe η^2+m theilbar durch δ, weshalb jedem von ihnen $\delta-1$, ihnen allen also $(\delta-1)^2$ Systeme x, η, z entsprechen; ist aber $\left(\frac{-m}{\delta}\right)=+1$, so wird für $\delta-3$ jener Werthe η^2+m nicht theilbar durch δ, was $(\delta-3)(\delta-1)$ Systeme x, η, z ergiebt, während η^2+m für zwei Werthe von η durch δ theilbar wird und jedem von ihnen $2\delta-1$ Systeme x, z entsprechen, sodass es in diesem Falle

$$2(2\delta-1)+(\delta-3)(\delta-1)$$

Systeme x, η, z giebt. Im Ganzen findet man demnach

wenn $\left(\frac{-m}{\delta}\right)=-1$ ist,

$$\delta-1+(\delta-1)^2=\delta(\delta-1),$$

wenn $\left(\frac{-m}{\delta}\right)=+1$ ist,

$$\delta-1+2(2\delta-1)+(\delta-3)(\delta-1)=\delta(\delta+1)$$

oder jederzeit

$$\delta\left(\delta+\left(\frac{-m}{\delta}\right)\right)=\delta\left(\delta+\left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\right)$$

der Zahl m entsprechende Restsysteme x, η, z (mod. δ). Da

m aber $\frac{\delta - 1}{2}$ verschiedene Reste bedeuten darf, findet sich eine Anzahl

$$\frac{\delta(\delta-1)}{2} \cdot \left(\delta + \left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\right)$$

(mod. δ) zulässiger Restsysteme x, η, z. —

Wenn man nun nach jedem der in Frage kommenden Moduln eins der zulässigen Restsysteme wählt, lässt sich ein entsprechendes Restsystem nach dem Modulus

$$\Pi' = 4\,\Pi(\omega^{i+1}) \cdot \Pi(r^{i+1}) \cdot \Pi(\delta) = \Omega \cdot \Pi$$

aufstellen, welches allen drei gestellten Anforderungen genügt. Demnach giebt es

$$12 \cdot \prod (\omega^2 - 1)(\omega - 1)\omega^{2i} \cdot \prod \tfrac{1}{2}(r^2 - 1)(r - 1) r^{2i}$$
$$\cdot \prod \tfrac{1}{2}\delta(\delta - 1)\left(\delta + \left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\right)$$

d. h. wenn $\varkappa$ die Anzahl der verschiedenen Primfaktoren von Δ bezeichnet

$$(39)\quad \begin{cases} \frac{12}{2^\varkappa} \cdot \frac{\Pi'^3}{4^3\Omega} \cdot \prod \left(1 - \frac{1}{\omega}\right)\left(1 - \frac{1}{\omega^2}\right) \cdot \prod \left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{r^2}\right) \\ \qquad \cdot \prod \left(1 - \frac{1}{\delta}\right)\left(1 + \left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\frac{1}{\delta}\right) \end{cases}$$

nach dem Modulus Π' incongruente und jenen drei Anforderungen genügende Restsysteme x, η, z. Heisst α, β, γ jedes dieser Restsysteme, so werden sämmtliche den genannten Anforderungen genügende x, η, z durch folgende Formeln gegeben:

$$(40)\quad x = \Pi' \cdot u + \alpha, \quad \eta = \Pi' \cdot v + \beta, \quad z = \Pi' \cdot w + \gamma.$$

Doch müssen sie bei der Summation (37) noch der Beschränkung

$$(41)\qquad xz - \eta^2 \overline{\gtrless} \Omega M$$

unterworfen werden und den Ungleichheiten (33) bezw. den Gleichheiten (35) genügen.

9. Um dem entsprechend die Doppelsumme in der Formel (37) zu ermitteln, zerlegen wir sie in Partialsummen, indem wir zunächst nur diejenigen ihrer Glieder zusammenfassen,

welche einem bestimmten der zulässigen Restsysteme (mod. Π') entsprechen.

Sei dann T die Anzahl derjenigen zulässigen Werthsysteme x, η, z, für welche keine der Gleichheiten (35), T' die Anzahl derjenigen, für welche eine derselben, T'' die Anzahl derer, für welche zwei von ihnen stattfinden, so hat die gedachte Partialsumme den Werth

$$T + \frac{1}{2} T' + \frac{1}{4} T''.$$

Setzt man aber

$$(42) \quad \begin{cases} x' = \dfrac{x}{\sqrt{\Omega M}} = \dfrac{\Pi'}{\sqrt{\Omega M}} \cdot u + \dfrac{\alpha}{\sqrt{\Omega M}}. \\ \eta' = \dfrac{\eta}{\sqrt{\Omega M}} = \dfrac{\Pi'}{\sqrt{\Omega M}} \cdot v + \dfrac{\beta}{\sqrt{\Omega M}} \\ z' = \dfrac{z}{\sqrt{\Omega M}} = \dfrac{\Pi'}{\sqrt{\Omega M}} \cdot w + \dfrac{\gamma}{\sqrt{\Omega M}} \end{cases}$$

und betrachtet x', η', z' als rechtwinklige Coordinaten eines Punktes, so ist offenbar T die Anzahl der Gitterpunkte des durch die Gleichungen (42) bestimmten parallelepipedischen Systems, welche im Innern des durch die Ungleichheiten

$$x'z' - \eta'^2 \gtreqless 1$$

$$x' > 0, \quad \eta' > 0, \quad z' > 0, \quad 2\eta' < x' < z'$$

begrenzten Raumes liegen, T' die Anzahl derjenigen, die auf einer der ebenen Grenzflächen desselben, T'' die Anzahl derer, die auf eine Kante der letzteren fallen. Nach dem schon in nr. 6 benutzten geometrischen Hilfssatze wird T bei unendlich wachsendem M unendlich werden wie $M^{3/2}$, T' und T'' dagegen höchstens wie M selbst, daher werden für $M = \infty$

$$\lim. \frac{T'}{M^{3/2}} = \lim. \frac{T''}{M^{3/2}} = 0$$

dagegen

$$\frac{\Pi'^3}{\Omega^{3/2}} \cdot \lim. \frac{T}{M^{3/2}}$$

gleich dem Inhalte jenes Raumes sein, dessen Werth sich gleich $\frac{\pi}{9}$ findet*).

---

*) Vgl. Analytische Zahlentheorie S. 454 u. ff.

Auf solche Weise ergiebt sich der Grenzwerth der betrachteten Partialsumme gleich

$$\frac{1}{2^\lambda}\cdot\frac{\Omega^{3/2}}{\Pi'^3}\cdot\frac{\pi}{9},$$

und, weil dieser Werth nichts an sich hat, was auf das besondere, die Partialsumme bestimmende Restsystem α, β, γ hinweist, so findet sich endlich

$$\text{(43)}\qquad \lim_{M=\infty}\frac{\Sigma(M'')}{M^{3/2}} = \frac{1}{2^\lambda}\cdot\frac{\Omega^{3/2}}{\Pi'^3}\cdot\frac{\pi}{9}\cdot \mathsf{B},$$

wenn zur Abkürzung der Ausdruck (39) mit B bezeichnet wird. Nach (32) giebt der gefundene Ausdruck zugleich auch den Grenzwerth der mit ϱ multiplicirten rechten Seite der Fundamentalgleichung (19), und somit gewinnt man durch Vergleichung mit dem Grenzwerthe (28) ihrer linken Seite folgendes Resultat:

$$\frac{4\pi}{3}\cdot\frac{\mathsf{A}}{\Omega^{1/2}\Delta}\cdot\frac{\mathsf{M}}{\Pi^3} = \frac{\pi}{9}\cdot\frac{\Omega^{3/2}}{2^\lambda\Pi'^3}\cdot\mathsf{B}$$

und hieraus nach Einsetzung der Werthe für A, B und einfachen Reduktionen nachstehenden allgemeinen Ausdruck für das Maass eines Geschlechts ternärer Formen mit ungeraden Invarianten Ω, Δ:

$$\text{(44)}\quad\begin{cases}\mathsf{M} = \dfrac{2+E}{24}\cdot\dfrac{\Omega\Delta}{2^{\varkappa+\lambda}}\cdot\prod\left(1-\dfrac{1}{r^2}\right)\\ \qquad\cdot\prod\left(1+\left(\dfrac{-\Delta f}{\omega}\right)\dfrac{1}{\omega}\right)\cdot\prod\left(1+\left(\dfrac{-\Omega\mathfrak{F}}{\delta}\right)\dfrac{1}{\delta}\right),\end{cases}$$

bis auf die Bezeichnung derselbe Ausdruck, welchen Eisenstein im Journal f. d. r. u. a. Math. 35 S. 128 ohne Beweis mitgetheilt hat. Die Formel (16) ist als besonderer Fall hierin enthalten; denn, da dort die Determinante D der ternären Formen ohne quadratischen Theiler angenommen worden ist, hat man $\Omega = 1$, $\Delta = D$, die Primfaktoren ω und r fallen aus, also wird $\lambda = 0$, und, da $-A''$ dort als quadratischer Rest (mod. D) angenommen wurde, hat man

$$\left(\frac{-\Omega\mathfrak{F}}{\delta}\right) = \left(\frac{-A''}{\delta}\right) = 1,$$

in Folge davon nach der Formel (41) des zweiten Capitels

$E = -1$, und die Formel (44) geht, wenn man die Primfaktoren δ wieder d nennt, in die folgende, mit (16) übereinstimmende über:

$$\frac{1}{24 \cdot 2^{\varkappa}} \prod (d+1). -$$

Stephen Smith, dem wir bei dieser Darstellung im wesentlichen gefolgt sind, giebt in seiner mehrfach erwähnten Arbeit noch eine zweite Methode zur Bestimmung der rechten Seite der Gleichung (19), die uns jedoch wegen der Umkehrung einer gewissen Doppelsummation nicht ganz unbedenklich erscheint. Einer anderen Methode, welche in mehrfacher Hinsicht bemerkenswerth ist, bedient sich Minkowski in seiner oben angeführten Preisarbeit, doch mag es genügen, hier auf diese Herleitung nur hinzuweisen, da die trotz mancher Abweichungen analoge Herleitung des Maasses für Formen mit einer beliebigen Anzahl von Unbestimmten, welche im zweiten Abschnitte ausführlich dargestellt wird, auch jene Methode in ihrer Grundlage ausreichend charakterisirt.

10. Aus der Formel (44) für das Maass eines Geschlechts ternärer Formen der Ordnung (Ω, Δ) lässt sich ohne weitere Schwierigkeit das Maass der Ordnung (Ω, Δ) selbst ermitteln, welches der Summe der Maasse sämmtlicher ihrer Geschlechter gleich ist. Nennt man das Maass der Ordnung $\mathfrak{M}$, so erhält man zunächst die Formel

$$\begin{aligned}\mathfrak{M} = \frac{\Omega\Delta}{24} \cdot \sum \Big[(2+E) \prod \tfrac{1}{4}\Big(1 - \tfrac{1}{r^2}\Big) \\ \cdot \prod \tfrac{1}{2}\Big(1 + \Big(\tfrac{-\Delta f}{\omega}\Big)\tfrac{1}{\omega}\Big) \\ \cdot \prod \tfrac{1}{2}\Big(1 + \Big(\tfrac{-\Omega \mathfrak{F}}{\delta}\Big)\tfrac{1}{\delta}\Big)\Big].\end{aligned}$$

Der Beziehung

$$E = (-1)^{\frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}} \cdot \Big(\frac{f}{\Omega}\Big) \cdot \Big(\frac{\mathfrak{F}}{\Delta}\Big)$$

zufolge lässt sie sich folgendermassen schreiben:

$$\mathfrak{M} = \frac{\Omega\Delta}{24}\Big(2R + (-1)^{\frac{\Omega+1}{2} \cdot \frac{\Delta+1}{2}} \cdot R'\Big), \tag{45}$$

wenn man mit R und R' die nachstehenden, über sämmtliche

Werthcombinationen der Symbole

$$\left(\frac{f}{r}\right),\ \left(\frac{\mathfrak{F}}{r}\right),\ \left(\frac{f}{\omega}\right),\ \left(\frac{\mathfrak{F}}{\delta}\right)$$

auszudehnenden Summenausdrücke

$$(46)\ \begin{cases} R = \sum\Big[\prod\frac{1}{4}\left(1-\frac{1}{r^2}\right)\cdot\prod\frac{1}{2}\left(1+\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right) \\ \qquad\qquad\cdot\prod\frac{1}{2}\left(1+\left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\frac{1}{\delta}\right)\Big] \end{cases}$$

$$(47)\ \begin{cases} R' = \sum\Big[\left(\frac{f}{\Omega}\right)\left(\frac{\mathfrak{F}}{\Delta}\right)\cdot\prod\frac{1}{4}\left(1-\frac{1}{r^2}\right) \\ \qquad\qquad\cdot\prod\frac{1}{2}\left(1+\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right) \\ \qquad\qquad\cdot\prod\frac{1}{2}\left(1+\left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\frac{1}{\delta}\right)\Big] \end{cases}$$

bezeichnet. Der Werth der letzteren ist unschwer anzugeben. Denn schreibt man zunächst in R das allgemeine Glied der Summe, indem man einen der Faktoren

$$\frac{1}{2}\left(1+\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right)$$

herausgreift und das Produkt aller übrigen kurz Π' nennt, folgendermassen:

$$\prod{}'\cdot\frac{1}{2}\left(1+\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right),$$

so entspricht diesem Gliede ein zweiter Summande

$$\prod{}'\cdot\frac{1}{2}\left(1-\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right),$$

und beide zusammen geben Π'; man darf also im Ausdruck (46) von R den betrachteten Faktor

$$\frac{1}{2}\left(1+\left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right)$$

unterdrücken, wenn man dann nur noch über die verschiedenen Werthcombinationen der übrigen Symbole summirt. Da ähnliches bezüglich der anderen Symbole $\left(\frac{f}{\omega}\right)$, sowie bezüglich der Symbole $\left(\frac{\mathfrak{F}}{\delta}\right)$ gilt, erhält man zunächst

$$R = \sum\prod\frac{1}{4}\left(1-\frac{1}{r^2}\right),$$

wo diese Summe nur noch über alle Werthcombinationen der Symbole $\left(\frac{f}{r}\right)$, $\left(\frac{\mathfrak{F}}{r}\right)$ ausgedehnt werden muss, und da jedem r vier solcher Combinationen entsprechen, überzeugt man sich durch die gleiche Betrachtung, dass schliesslich

$$(48)\qquad R = \prod\left(1 - \frac{1}{r^2}\right)$$

ist.

Man betrachte zweitens R'. Wenn man mit Ω_1, Δ_1 diejenigen Quotienten bezeichnet, welche aus Ω, Δ durch Division mit den grössten darin aufgehenden Quadratzahlen entstehen, so kann

$$\left(\frac{f}{\Omega}\right)\cdot\left(\frac{\mathfrak{F}}{\Delta}\right) \text{ durch } \left(\frac{f}{\Omega_1}\right)\cdot\left(\frac{\mathfrak{F}}{\Delta_1}\right)$$

ersetzt werden. Ist dann ω ein Primfaktor von Ω, der nicht in Ω_1, oder δ ein Primfaktor von Δ, der nicht in Δ_1 aufgeht, so lehrt die bei R angewandte Schlussweise offenbar, dass der betreffende Faktor

$$\frac{1}{2}\left(1 + \left(\frac{-\Delta f}{\omega}\right)\frac{1}{\omega}\right) \quad \text{resp.} \quad \frac{1}{2}\left(1 + \left(\frac{-\Omega\mathfrak{F}}{\delta}\right)\frac{1}{\delta}\right)$$

im Ausdrucke von R' unterdrückt werden darf, wenn dann die Summation nur noch auf die übrigen Symbole erstreckt wird. Ist jedoch ω ein Primfaktor von Ω_1, so kann das allgemeine Glied der noch auszuführenden Summation in der Form

$$\prod{}' \cdot \frac{1}{2}\left(\left(\frac{f}{\omega}\right) + \left(\frac{-\Delta}{\omega}\right)\frac{1}{\omega}\right)$$

geschrieben werden, wo Π' unabhängig ist von ω, und es entspricht ihm ein zweites Glied

$$\prod{}' \cdot \frac{1}{2}\left(-\left(\frac{f}{\omega}\right) + \left(\frac{-\Delta}{\omega}\right)\frac{1}{\omega}\right),$$

welches, mit ihm vereint, einfach

$$\prod{}' \cdot \left(\frac{-\Delta}{\omega}\right)\frac{1}{\omega}$$

giebt. Der bezügliche Faktor

$$\frac{1}{2}\left(\left(\frac{f}{\omega}\right) + \left(\frac{-\Delta}{\omega}\right)\frac{1}{\omega}\right)$$

darf demnach im Ausdrucke von R' unterdrückt werden, wenn die Summation dann nur noch auf die übrigen Symbole bezogen und vor der Summe mit $\left(\frac{-\varDelta}{\omega}\right)\frac{1}{\omega}$ multiplicirt wird. Bezüglich der anderen Primfaktoren von Ω_1 sowie der Primfaktoren von $\varDelta_1$ lässt sich ähnliches bemerken, sodass die alsdann verbleibende Summation sich nur noch auf die verschiedenen Werthcombinationen der Symbole $\left(\frac{f}{r}\right)$, $\left(\frac{\mathfrak{F}}{r}\right)$ bezieht. Bedeutet aber r einen in Ω_1 aufgehenden Primfaktor, so würde dem allgemeinen Gliede jener Summe, das sich in der Gestalt

$$\prod{}' \cdot \frac{1}{4}\left(\frac{f}{r}\right) \cdot \left(1 - \frac{1}{r^2}\right)$$

schreiben lässt, während Π' von $\left(\frac{f}{r}\right)$ unabhängig ist, ein zweites

$$-\prod{}' \cdot \frac{1}{4}\left(\frac{f}{r}\right) \cdot \left(1 - \frac{1}{r^2}\right)$$

entsprechen, das jenes aufhebt, und R' würde Null. Dasselbe würde der Fall sein, wenn r in $\varDelta_1$ aufginge, und man findet folglich

(49a) $$R' = 0,$$

so oft eine im grössten gemeinsamen Theiler von Ω, $\varDelta$ aufgehende Primzahl auch in $\Omega_1 \cdot \varDelta_1$ aufgeht, d. i. so oft $\Omega_1 \cdot \varDelta_1$ nicht prim ist gegen den grössten gemeinsamen Theiler von $\Omega, \varDelta$.

Falls aber kein r in $\Omega_1 \cdot \varDelta_1$ aufgeht, so ergiebt sich, ganz wie bei R,

$$R' = \prod\left(1 - \frac{1}{r^2}\right) \cdot \prod\left(\frac{-\varDelta}{\omega}\right)\frac{1}{\omega} \cdot \prod\left(\frac{-\Omega}{\delta}\right)\frac{1}{\delta},$$

wo die letzteren beiden Produkte über alle Primfaktoren von $\Omega_1, \varDelta_1$ auszudehnen sind; in dem, dem vorigen entgegengesetzten Falle ist also

$$R' = \left(\frac{-\varDelta}{\Omega_1}\right) \cdot \left(\frac{-\Omega}{\varDelta_1}\right)\frac{1}{\Omega_1 \varDelta_1} \cdot \prod\left(1 - \frac{1}{r^2}\right)$$

oder auch

(49b) $$R' = -\frac{(-1)^{\frac{\Omega+1}{2}\cdot\frac{\varDelta+1}{2}}}{\Omega_1 \varDelta_1} \cdot \prod\left(1 - \frac{1}{r^2}\right).$$

Führt man die so gefundenen Werthe von R und R' in die Formel (45) ein und setzt

$$\lambda = \frac{1}{\Omega_1 \Delta_1} \quad \text{oder } \lambda = 0,$$

jenachdem $\Omega_1 \Delta_1$ prim ist gegen den grössten gemeinsamen Theiler von Ω und Δ oder nicht, so erhält man folgenden Ausdruck für das Maass der Ordnung (Ω, Δ):

$$(50) \qquad \mathfrak{M} = \frac{\Omega \Delta}{24}(2 - \lambda) \cdot \prod \left(1 - \frac{1}{r^2}\right). -$$

Smith hat in seiner Arbeit auch den allgemeinen Ausdruck dieses Maasses mitgetheilt, wie er irgendwelchen Werthen der Invarianten Ω, Δ und nicht nur eigentlich- sondern auch uneigentlich-primitiven Formen entspricht. Diese allgemeine Formel lautet:

$$\mathfrak{M} = \frac{\Omega \Delta}{8} \cdot Z \cdot \prod \left(1 - \frac{1}{r^2}\right).$$

Zur Bestimmung des Faktors Z je nach den verschiedenen möglichen Fällen dienen die nachstehenden Tabellen, welche jener Arbeit entnommen sind; J_1 und J_2 bedeuten darin die Exponenten der höchsten Potenzen von 2, welche resp. in Ω und Δ enthalten sind.

I. Wenn f und $\mathfrak{F}$ eigentlich-primitiv sind:

	$J_1 = 0$	J_1 gerade	J_1 ungerade
$J_2 = 0$	$Z = \frac{1}{3}(2 - \lambda)$	$\frac{1}{4}(2 - \lambda)$	$\frac{1}{2}$
J_2 gerade	$\frac{1}{4}(2 - \lambda)$	$\frac{1}{4}(2 - \lambda)$	$\frac{1}{2}$
J_2 ungerade	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

II. Wenn f uneigentlich-, $\mathfrak{F}$ eigentlich-primitiv sind:

$$J_1 = 0, \quad J_2 > 0$$

$$J_2 \text{ gerade:} \quad Z = \frac{1}{12}(2 - \lambda)$$

$$J_2 \text{ ungerade:} \quad Z = \frac{1}{6}(1 - \lambda)$$

III. Wenn f eigentlich-, $\mathfrak{F}$ uneigentlich-primitiv sind:

$$J_1 > 0, \quad J_2 = 0.$$

$$J_1 \text{ gerade:} \quad Z = \frac{1}{12}(2 - \lambda)$$

$$J_1 \text{ ungerade:} \quad Z = \frac{1}{6}(1 - \lambda). \text{ —}$$

Die Formel (50) findet sich bereits richtig angegeben bei Eisenstein (Neue Theoreme der höheren Arithmetik, J. f. d. r. u. a. Math. 35), jedoch, wie Smith angemerkt hat, mit einer näheren Erklärung, welche nicht ganz richtig ist. Nennt man nämlich R den grössten gemeinsamen Theiler von

$$\Omega = \Omega_1 \cdot \Omega_2^2 \quad \text{und} \quad \Delta = \Delta_1 \cdot \Delta_2^2,$$

und Q das grösste in $\Omega\Delta$ aufgehende Quadrat, so soll nach Eisenstein $\lambda = 0$ sein, wenn R keine Quadratzahl, dagegen $\lambda = \frac{Q}{\Omega\Delta}$, wenn R Quadratzahl ist. Dies ist aber etwas anderes, als was nach obiger Herleitung für λ gilt. Denn, heisst

D_1	der	grösste	gem.	Theiler	von	Ω_1, Δ_1
D_2	"	"	"	"	"	Ω_2, Δ_2
d	"	"	"	"	"	$\frac{\Omega_1}{D_1}, \frac{\Delta_2}{D_2}$
δ	"	"	"	"	"	$\frac{\Delta_1}{D_1}, \frac{\Omega_2}{D_2}$,

so findet sich, wie leicht zu übersehen,

$$R = d\delta D_1 \cdot D_2^2$$

$$\frac{Q}{\Omega\Delta} = \frac{D_1^2}{\Omega_1 \Delta_1}.$$

Demnach ist R dann und nur dann ein Quadrat, wenn es

$$d\delta D_1 \; .$$

d. h., wenn

$$d = \delta = D_1 = 1$$

ist. Dagegen ist $\Omega_1 \Delta_1$ prim gegen R dann und nur dann, wenn ausser

$$d = \delta = D_1 = 1$$

noch $\Omega_1 \Delta_1$ prim zu D_2 ist. Folglich ist zwar R, so oft letzteres der Fall ist, ein Quadrat und dann stimmt $\frac{Q}{\Omega\Delta}$ mit

dem nach Smith angegebenen Werthe von λ überein, aber nicht umgekehrt. In Wahrheit ist λ nur dann nicht Null, wenn der Exponent jedes gemeinsamen Primfaktors von Ω und Δ sowohl in Ω als in Δ gerade ist.

Achtes Capitel.

Unbestimmte Formen. Die Gleichung $ax^2 + a'x'^2 + a''x''^2 = 0$.

1. Wir wenden uns nunmehr von den positiven (bestimmten) zu den unbestimmten ternären Formen, müssen jedoch von vornherein bemerken, dass deren Theorie vielfach grössere Schwierigkeiten darbietet und deshalb auch noch nicht mit gleichem Erfolge bearbeitet worden ist, wie jene. Nur von einzelnen sie betreffenden Fragen werden wir berichten können, die man bereits erledigt oder doch wenigstens nicht ohne Erfolg in Angriff genommen hat. Zu diesen gehört die ganzzahlige Auflösung der Gleichung

$$(1) \qquad ax^2 + a'x'^2 + a''x''^2 = 0,$$

und wir wollen zunächst die Bedingungen feststellen, unter denen diese Gleichung mittels ganzer Zahlen auflösbar ist.

Jedenfalls dürfen die Coefficienten a, a', a'' nicht sämmtlich dasselbe Vorzeichen haben, denn andernfalls könnte die Gleichung keine Lösung haben ausser der selbstverständlichen Lösung

$$x = 0, \quad x' = 0, \quad x'' = 0,$$

von welcher hinfort stets abgesehen werden soll.

Bevor wir weiter auf diese Frage eingehen, mag bemerkt werden, dass auf die Gleichung (1) die allgemeinere:

$$(2) \quad f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx' = 0$$

zurückkommt. In der That, durch f können keine anderen Zahlen dargestellt werden, als durch irgend eine mit f äqui-

valente Form f', und die Darstellungen einer bestimmten Zahl z. B. der Null, durch die eine von ihnen ergeben sich stets auf einfache Weise aus ihren Darstellungen durch die andere, man kann daher die Auflösung der Gleichung (2) auf die der Gleichung $f' = 0$ zurückführen. Nun lässt sich (vgl. nr. 11 des zweiten Capitels) eine zu f äquivalente Form f' finden, in welcher der erste Coefficient ebenso wie der dritte Coefficient in ihrer Adjungirten von Null verschieden ist, d. h. bei Auflösung der Gleichung (2) darf man sich auf den Fall beschränken, wo a und A'' von Null verschieden sind. In ihm ist aber die aufzulösende Gleichung gleichbedeutend mit der anderen:

$$(3) \qquad A''(ax + b''x' + b'x'')^2 + (A''x' - Bx'')^2 + aDx''^2 = 0,$$

welche aus ihr durch Multiplikation mit aA'' entsteht. Sie würde mithin, sobald die Form f eine bestimmte ist, A'' und aD also positiv sind, nur erfüllt werden können, indem man

$$ax + b''x' + b'x'' = 0, \quad A''x' - Bx'' = 0, \quad x'' = 0$$

setzt, d. i. durch die evidente Lösung

$$x = x' = x'' = 0.$$

Nimmt man daher die Form f als eine unbestimmte an, so erhält die Gleichung (3) die Gestalt

$$(4) \qquad A''y^2 + y'^2 + aDy''^2 = 0,$$

in welcher die Coefficienten nicht alle gleiches Vorzeichen haben, d. h. man kommt auf eine Gleichung von der Gestalt (1) zurück, wenn man

$$ax + b''x' + b'x'' = y, \quad A''x' - Bx'' = y', \quad x'' = y''$$

setzt; und offenbar erhält man aus allen rationalen Lösungen y, y', y'' der Gleichung (4) sämmtliche rationale Lösungen x, x', x'' der Gleichung (1) und umgekehrt. Kennt man aber alle rationalen Lösungen einer homogenen Gleichung, so kennt man damit implicite auch ihre ganzzahligen Lösungen.

Nach dieser Vorbemerkung dürfen wir uns fortan auf die einfachere Gleichung (1) beschränken.

2. Diese Gleichung behält offenbar dieselben Lösungen, wenn man den etwa vorhandenen gemeinsamen Theiler von a, a', a'' unterdrückt, demnach dürfen a, a', a'' frei von

jedem, von 1 verschiedenen gemeinsamen Theiler vorausgesetzt werden. Sei dann

$$a = bp^2, \quad a' = b'p'^2, \quad a'' = b''p''^2,$$

wo p^2, p'^2, p''^2 die grössten in a, a', a'' aufgehenden Quadratzahlen bezeichnen.

Aus der Gleichung (1) folgt die andere:

$$b(px)^2 + b'(p'x')^2 + b''(p''x'')^2 = 0,$$

d. h. aus jeder ganzzahligen Auflösung von (1) folgt eine ganzzahlige Auflösung der Gleichung

$$bx^2 + b'x'^2 + b''x''^2 = 0, \tag{5}$$

deren Coefficienten keinen quadratischen Theiler mehr haben. Und umgekehrt schliesst man aus der letzteren durch Multiplikation mit $p^2 p'^2 p''^2$ die Gleichung

$$a(p'p''x)^2 + a'(p''px')^2 + a''(pp'x'')^2 = 0,$$

also folgt auch aus jeder ganzzahligen Lösung von (5) eine solche von (1). Die beiden Gleichungen (1) und (5) sind also gleichzeitig in ganzen Zahlen auflösbar oder gleichzeitig nicht auflösbar. Bei der Frage nach der Auflösbarkeit der Gleichung (1) darf man sich also weiter auf den Fall beschränken, dass die Coefficienten a, a', a'' ausser der bereits gemachten die Voraussetzung erfüllen, ohne quadratische Theiler zu sein.

Ist dann

α der grösste gemeinsame Theiler von a', a''
α' „ „ „ „ „ a'', a
α'' „ „ „ „ „ a, a',

so sind $\alpha^2, \alpha'^2, \alpha''^2$ die grössten Quadrate, welche resp. in den Produkten $a'a''$, $a''a$, aa' aufgehen; ferner sind $\alpha, \alpha', \alpha''$ zu je zweien relativ prim, denn hätten z. B. α', α'' einen gemeinsamen Primtheiler, so würde er wegen α' in a'' und a, wegen α'' in a und a' aufgehen, also allen drei Coefficienten a, a', a'' gemeinsam sein, gegen die Voraussetzung. Da aber a sowohl durch α' als durch α'' theilbar ist, ist es auch theilbar durch $\alpha'\alpha''$ und man findet die erste der folgenden drei Gleichungen, von denen die anderen auf analoge Weise hervorgehen:

$$a=\alpha'\alpha''\cdot b,\quad a'=\alpha''\alpha\cdot b'\quad a''=\alpha\alpha'\cdot b'',$$

und in denen unter b, b', b'' drei ganze Zahlen ohne gemeinsamen und ohne quadratischen Theiler zu verstehen sind. Setzt man hier

$$\alpha b=\mathfrak{a},\quad \alpha' b'=\mathfrak{a}',\quad \alpha'' b''=\mathfrak{a}'',$$

so nehmen die Gleichungen die neue Gestalt an:

$$a\alpha=\alpha'\alpha''\cdot\mathfrak{a},\quad a'\alpha'=\alpha''\alpha\cdot\mathfrak{a}',\quad a''\alpha''=\alpha\alpha'\cdot\mathfrak{a}''.$$

Da $\frac{a'a''}{\alpha^2}=\mathfrak{a}'\mathfrak{a}''$ keinen quadratischen Theiler hat, müssen $\mathfrak{a}'$, $\mathfrak{a}''$ — und allgemeiner je zwei der Zahlen $\mathfrak{a}, \mathfrak{a}', \mathfrak{a}''$ relativ prim sein.

Dies vorausgeschickt, folgt nun aus Gleichung (1) durch Multiplikation mit $\alpha^2\alpha'^2\alpha''^2$

$$a\alpha^2\cdot(\alpha'\alpha''x)^2+a'\alpha'^2\cdot(\alpha''\alpha x')^2+a''\alpha''^2\cdot(\alpha\alpha'x'')^2=0$$

d. i.

$$\alpha\alpha'\alpha''\cdot[\mathfrak{a}(\alpha'\alpha''x)^2+\mathfrak{a}'\cdot(\alpha''\alpha x')^2+\mathfrak{a}''\cdot(\alpha\alpha'x'')^2]=0$$

also aus einer ganzzahligen Lösung von (1) auch eine ganzzahlige Lösung der Gleichung

$$\mathfrak{a}x^2+\mathfrak{a}'x'^2+\mathfrak{a}''x''^2=0;\tag{6}$$

und umgekehrt folgt aus dieser durch Multiplikation mit $\alpha\alpha'\alpha''$

$$a(\alpha x)^2+a'(\alpha'x')^2+a''(\alpha''x'')^2=0$$

d. i. aus einer ganzzahligen Lösung von (6) auch eine solche von (1). Beide Gleichungen sind mithin gleichzeitig lösbar oder gleichzeitig nicht lösbar, und folglich dürfen bei der Frage nach der Auflösbarkeit der Gleichung (1) die Coefficienten a, a', a'' zu je zweien relativ prim vorausgesetzt werden, ohne die früheren Annahmen preiszugeben.

So sei denn also vorausgesetzt, dass in der Gleichung (1) die Coefficienten a, a', a'' zu je zweien relativ prim und ohne quadratische Theiler sind. Auch darf man die Gleichung (1) mit solchem Vorzeichen nehmen, dass $D=aa'a''$ positiv ist.

Nun erhält man die sämmtlichen ganzzahligen Auflösungen x, x', x'' dieser Gleichung aus den eigentlichen d. i. denjenigen, welche ohne einen von 1 verschiedenen gemeinsamen Theiler sind, indem man die letzteren mit jeder be-

liebigen ganzen Zahl zugleich multiplicirt. Fragt man daher nach den nothwendigen und hinreichenden Bedingungen für die Auflösbarkeit der Gleichung (1), so darf man die Frage bestimmter so fassen: Wann hat diese Gleichung eigentliche Auflösungen? Unter den gemachten Voraussetzungen sind letztere auch zu je zweien relativ prim; denn ein gemeinschaftlicher Primtheiler p von x', x'' z. B. würde einen quadratischen Theiler p^2 von ax^2 liefern, also, da a keinen solchen besitzt, auch in x aufgehen müssen. Für eigentliche Auflösungen x, x', x'' sind sogar auch $ax, a'x', a''x''$ zu je zweien relativ prim, denn ein gemeinsamer Primtheiler von $a'x', a''x''$ z. B. müsste auch aufgehen in ax und, weil er höchstens in einer der Zahlen x, x', x'' aufgehen kann, müsste er in mindestens zwei der Zahlen a, a', a'' aufgehen, gegen die Voraussetzung. Dass auch umgekehrt eine Lösung, für welche ax, $a'x'$, $a''x''$ zu zweien prim sind, eine eigentliche ist, geht unmittelbar daraus hervor, dass dann auch x, x', x'' zu zweien relativ prim sein müssen.

Die erschöpfende Antwort auf die gestellte Frage gab zuerst Legendre*), indem er folgenden Satz bewies: Unter den für die Coefficienten a, a', a'' geltenden Voraussetzungen ist es zur ganzzahligen Auflösbarkeit der Gleichung (1) nothwendig und hinreichend, dass

$$-a'a'', \quad -a''a, \quad -aa'$$

resp. von a, a', a'' quadratische Reste sind. Das Verfahren, mittels dessen Legendre diesen Satz herleitete, rührt von Lagrange her**) und besteht im Wesentlichen darin, die Gleichung (1) zunächst durch eine andere von der Form

$$x^2 = Ay^2 + Bz^2$$

zu ersetzen und die Frage nach der Auflösbarkeit der letzteren zurückzuführen auf die gleiche Frage für eine Gleichung derselben Form

$$x^2 = A'y^2 + B'z^2,$$

---

*) In hist. de l'Acad. de Paris 1784, p. 507, sowie in seiner théorie des nombres 3. éd. t. 1 §§ 3 und 4.

**) S. Mém. de l'Acad. de Berlin für das Jahr 1767, sowie auch § V der Additions zu Euler's élémens d'algèbre.

in welcher $A'B' < AB$ ist, u. s. w. Dieses Beweisverfahren ist in neuer Zeit von Dedekind sehr vereinfacht worden*). Gleichwohl soll hier auf diesen Beweis, ohne ihn zur Darstellung zu bringen, nur verwiesen und statt seiner derjenige entwickelt werden, welchen man Gauss verdankt**), weil dieser unmittelbar aus der Theorie der ternären quadratischen Formen geschöpft ist, zu welcher die Frage ihrer wesentlichen Natur nach gehört.

3. Wenn eine eigentliche Lösung x, x', x'' der Gleichung (1) vorhanden ist, so sind, wie bemerkt, ax, $a'x'$, $a''x''$ zu je zweien relativ prim und folglich werden sich drei ganze Zahlen $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ bestimmen lassen, welche den Congruenzen

$$(7)\qquad \begin{cases} \mathfrak{A}x'' \equiv a'x' \pmod{a} \\ \mathfrak{A}'x \equiv a''x'' \pmod{a'} \\ \mathfrak{A}''x' \equiv ax \pmod{a''} \end{cases}$$

Genüge leisten; in Folge der Congruenzen, welche sich aus der Gleichung (1) ergeben, wenn sie (mod. a, a', a'') aufgefasst wird, findet sich dann ohne weiteres, dass die Zahlen $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ auch folgende Congruenzen erfüllen:

$$(8)\qquad \begin{cases} \mathfrak{A}^2 \equiv -a'a'' \pmod{a} \\ \mathfrak{A}'^2 \equiv -a''a \pmod{a'} \\ \mathfrak{A}''^2 \equiv -aa' \pmod{a''} \end{cases}$$

und folglich müssen $-a'a''$, $-a''a$, $-aa'$ resp. von a, a', a'' quadratische Reste sein, damit die Gleichung (1) auflösbar ist.

Es gilt nun, das Umgekehrte zu beweisen. Um dieser Umkehrung sogleich ihren vollen Umfang zu geben, schicken wir einige Bemerkungen vorauf.

Man nenne $\alpha, \alpha', \alpha''$ die Anzahl der verschiedenen Primzahlen, aus denen a, a', a'' bestehen und also $\theta = \alpha + \alpha' + \alpha''$ die Anzahl derjenigen, aus welchen die Determinante $D = aa'a''$ der Form

*) In den Vorlesungen über Zahlentheorie von Dirichlet, herausgegeben von Dedekind, 4. Aufl. S 428.

**) Gauss in Disquis. Arithm. 294. Vgl. G. Cantor, de aequationibus 2. gradus indeterminatis, Inauguraldissertation, Berlin 1867, § 8.

$$ax^2 + a'x'^2 + a''x''^2$$

zusammengesetzt ist; ist alsdann zunächst D ungerade, so werden die Congruenzen (8), wenn sie überhaupt möglich sind, $2^\alpha, 2^{\alpha'}, 2^{\alpha''}$ Wurzeln haben und demnach 2^ϱ verschiedene Systeme solcher Wurzeln $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ vorhanden sein. Für eine gerade Determinante D muss einer der Moduln a, a', a'', z. B. der erste, gerade sein; da jedoch a nach Voraussetzung keinen quadratischen Theiler hat, kann es nur durch die erste Potenz von 2 theilbar sein und somit hat dann die erste Congruenz (8), wenn sie lösbar ist, wieder nur genau 2^α Wurzeln, die Anzahl der Wurzelsysteme $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ beträgt also auch in diesem Falle 2^ϱ. — Die Umkehrung, die bewiesen werden soll, kann nun folgendermassen gefasst werden: Sind $-a'a''$, $-a''a$, $-aa'$ resp. von a, a', a'' quadratische Reste, so giebt es für jede der Wurzelcombinationen $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ der Congruenzen (8) eine eigentliche Lösung x, x', x'' der Gleichung (1), welche den Congruenzen (7) Genüge leistet.

Um sich hiervon zu überzeugen, betrachte man irgend eine der Wurzelcombinationen $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$. Man kann dann, da die Zahlen a, a', a'' relativ prim sind, immer ganze Zahlen X, X', X'' den folgenden Congruenzen gemäss wählen:

$$(9)\quad \begin{cases} X \equiv a'' \pmod{a'}, & X \equiv \mathfrak{A}'' \pmod{a''} \\ X' \equiv a \pmod{a''}, & X' \equiv \mathfrak{A} \pmod{a} \\ X'' \equiv a' \pmod{a}, & X'' \equiv \mathfrak{A}' \pmod{a'}. \end{cases}$$

Für diese so gewählten Zahlen wird dann

$$(10)\qquad aX^2 + a'X'^2 + a''X''^2 \equiv 0 \pmod{D}$$

sein, da diese Congruenz nach jedem der Moduln a, a', a'' besteht; in der That hat man z. B.

$$aX^2 + a'X'^2 + a''X''^2 \equiv a' \cdot \mathfrak{A}^2 + a'' \cdot a'^2 \equiv 0 \pmod{a}$$

u. s. w. Ferner ist zufolge der Congruenzen (9) X prim sowohl zu a' wie zu a'', da sonst a' und a'' oder aa' und a'' einen gemeinsamen Theiler hätten; gleicherweise ist X' prim zu a'' und zu a, X'' prim gegen a und a'. Aus diesem Grunde muss jeder etwa vorhandene gemeinsame Theiler von X, X', X''

prim sein gegen D. Nennt man also d ihren grössten gemeinsamen Theiler, setzt

$$X = d\mathfrak{x}, \quad X' = d\mathfrak{x}', \quad X'' = d\mathfrak{x}''$$

und bestimmt δ durch die Congruenz $d\delta \equiv 1 \pmod{D}$, so nehmen die Congruenzen (9) und (10) folgende Gestalt an:

$$(11) \qquad \begin{cases} \mathfrak{x} \equiv a''\delta \pmod{a'}, & \mathfrak{x} \equiv \mathfrak{A}''\delta \pmod{a''} \\ \mathfrak{x}' \equiv a\delta \pmod{a''}, & \mathfrak{x}' \equiv \mathfrak{A}\delta \pmod{a} \\ \mathfrak{x}'' \equiv a'\delta \pmod{a}, & \mathfrak{x}'' \equiv \mathfrak{A}'\delta \pmod{a'} \end{cases}$$

und

$$(12) \qquad a\mathfrak{x}^2 + a'\mathfrak{x}'^2 + a''\mathfrak{x}''^2 \equiv 0 \pmod{D}.$$

Nun haben aber die drei Zahlen $a\mathfrak{x}, a'\mathfrak{x}', a''\mathfrak{x}''$ keinen gemeinsamen Theiler, denn ein solcher müsste, da er in $a'\mathfrak{x}'$ und $a''\mathfrak{x}''$ aufginge, prim sein gegen a, und in gleicher Weise gegen a' und a'', er müsste also $\mathfrak{x}, \mathfrak{x}', \mathfrak{x}''$ gemeinsam sein, gegen die Bedeutung dieser Zeichen. In Folge hiervon giebt es ganze Zahlen $\lambda, \lambda', \lambda''$, welche die Gleichung

$$a\mathfrak{x} \cdot \lambda + a'\mathfrak{x}' \cdot \lambda' + a''\mathfrak{x}'' \cdot \lambda'' = 1$$

erfüllen, und ferner nach dem Gauss'schen Hilfssatze sechs ganze Zahlen, für welche

$$\mu'\nu'' - \mu''\nu' = a\mathfrak{x}, \quad \mu''\nu - \mu\nu'' = a'\mathfrak{x}', \quad \mu\nu' - \mu'\nu = a''\mathfrak{x}''$$

ist. Durch die Substitution

$$(13) \qquad \begin{cases} x = \lambda y + \mu y' + \nu y'' \\ x' = \lambda' y + \mu' y' + \nu' y'' \\ x'' = \lambda'' y + \mu'' y' + \nu'' y'' \end{cases}$$

mit dem Modulus 1 geht alsdann die Formel

$$ax^2 + a'x'^2 + a''x''^2$$

in eine äquivalente Form

$$g = \begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$$

über. Nennt man

$$\begin{aligned} y &= a\mathfrak{x} \cdot x + a'\mathfrak{x}' \cdot x' + a''\mathfrak{x}'' \cdot x'' \\ y' &= \eta \cdot x + \eta' \cdot x' + \eta'' \cdot x'' \\ y'' &= \zeta \cdot x + \zeta' \cdot x' + \zeta'' \cdot x'' \end{aligned}$$

die umgekehrte Substitution (13), so findet sich nach einfachen Determinantensätzen

$$(14)\quad \begin{cases} \mu = a''\xi''\zeta' - a'\xi'\zeta'', & \nu = a'\xi'\eta'' - a''\xi''\eta' \\ \mu' = a\xi\zeta'' - a''\xi''\zeta, & \nu' = a''\xi''\eta - a\xi\eta'' \\ \mu'' = a'\xi'\zeta - a\xi\zeta', & \nu'' = a\xi\eta' - a'\xi'\eta. \end{cases}$$

Mit Rücksicht hierauf nehmen die Beziehungen

$$\begin{aligned} m' &= a\mu^2 + a'\mu'^2 + a''\mu''^2 \\ m'' &= a\nu^2 + a'\nu'^2 + a''\nu''^2 \\ n &= a\mu\nu + a'\mu'\nu' + a''\mu''\nu'', \end{aligned}$$

welche zwischen den Coefficienten m', n, m'' der neuen und den Coefficienten der ursprünglichen Form bestehen, wenn sie als Congruenzen (mod. a) aufgefasst werden, die Gestalt an:

$$\left.\begin{aligned} m' &\equiv a'a''\zeta^2(a'\xi'^2 + a''\xi''^2) \equiv 0 \\ m'' &\equiv a'a''\eta^2(a'\xi'^2 + a''\xi''^2) \equiv 0 \\ n &\equiv - a'a''\zeta\eta(a'\xi'^2 + a''\xi''^2) \equiv 0 \end{aligned}\right\} \text{(mod. } a),$$

d. h. m', n, m'' sind theilbar durch a; und weil in gleicher Weise Gleiches in Bezug auf a' und a'' gefunden wird, so sind m', n, m'' theilbar durch D. Setzt man demgemäss

$$m' = DM', \quad n = DN, \quad m'' = DM''$$

und ferner

$$Dm = M, \quad n' = N', \quad n'' = N'',$$

so sieht man sogleich, dass $ax^2 + a'x'^2 + a''x''^2$ durch die Substitution

$$(15)\quad \begin{cases} x = D\lambda y + \mu y' + \nu y'' \\ x' = D\lambda' y + \mu' y' + \nu' y'' \\ x'' = D\lambda'' y + \mu'' y' + \nu'' y'' \end{cases}$$

mit dem Modulus D in die Form

$$D \cdot \begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$$

übergeht. Die Determinante der letzteren muss gleich D^3 und also diejenige der offenbar unbestimmten Form

$$G = \begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$$

gleich 1 sein; die Form G ist also (s. nr. 5 des fünften Cap.) der Form

$$2zz''-z'^2$$

äquivalent und geht in sie durch eine unimodulare Substitution

$$(16)\qquad \begin{cases} y=\varrho z+\sigma z'+\tau z'' \\ y'=\varrho' z+\sigma' z'+\tau' z'' \\ y''=\varrho'' z+\sigma'' z'+\tau'' z'' \end{cases}$$

über. Hier bemerke man sogleich, dass ein gemeinsamer Theiler der Elemente ϱ', ϱ'' nicht auch gleichzeitig ein solcher von τ', τ'' sein kann, da er sonst auch in $\sigma'\tau''-\sigma''\tau'$ und somit im Modulus 1 der Substitution aufgehen würde; wären also ϱ', ϱ'' insbesondere beide gerade, so könnten es nicht τ', τ'' beide sein, und umgekehrt. Bei der Symmetrie mit Bezug auf z und z'' darf man also im Folgenden voraussetzen, dass ϱ', ϱ'' nicht beide gerade sind. Alsdann lässt sich das bereits erlangte Ergebniss folgendermassen fassen:

Durch die Substitution

$$(17)\qquad \begin{cases} y=\varrho z+2\sigma z'+2\tau z'' \\ y'=\varrho' z+2\sigma' z'+2\tau' z'' \\ y''=\varrho'' z+2\sigma'' z'+2\tau'' z'' \end{cases}$$

mit dem Modulus 4 geht die Form G in die Form

$$4(zz''-z'^2)$$

über. Die aus (15) und (17) zusammengesetzte Substitution, deren Modulus $4D$ ist und der man die Form geben kann

$$(18)\qquad \begin{cases} x=\alpha z+\beta z'+\gamma z'' \\ x'=\alpha' z+\beta' z'+\gamma' z'' \\ x''=\alpha'' z+\beta'' z'+\gamma'' z'' \end{cases}$$

führt demnach die Form $ax^2+a'x'^2+a''x''^2$ in die Form $4D(zz''-z'^2)$ über.

Hieraus erhält man die Gleichung

$$a\alpha^2+a'\alpha'^2+a''\alpha''^2=0$$

d. i. eine Lösung der Gleichung (1):

$$x=\alpha,\ x'=\alpha',\ x''=\alpha'';$$

und diese kann nicht die evidente Lösung

$$\alpha = \alpha' = \alpha'' = 0$$

sein, da der Modulus der Substitution (18) von Null verschieden ist.

Für die Zahlen $\alpha, \alpha', \alpha''$ erhält man aber aus der Zusammensetzung von (15) und (17) die Bestimmung:

$$(19)\qquad \begin{cases} \alpha \;= D\lambda\varrho \;+ \mu\varrho' \;+ \nu\varrho'' \\ \alpha' \;= D\lambda'\varrho + \mu'\varrho' + \nu'\varrho'' \\ \alpha'' = D\lambda''\varrho + \mu''\varrho' + \nu''\varrho'', \end{cases}$$

vermöge deren man sich nun leicht überzeugt, dass die gefundene Lösung

$$x = \alpha,\; x' = \alpha',\; x'' = \alpha''$$

die Congruenzen (7) erfüllt. In der That nimmt nach Einsetzung derselben die erste der genannten Congruenzen die Gestalt an:

$$(20)\qquad \mathfrak{A}(\mu''\varrho' + \nu''\varrho'') \equiv a'(\mu'\varrho' + \nu'\varrho'') \pmod{a};$$

mit Rücksicht auf die Beziehungen (11) und (14) ergiebt sich jedoch

$$\left.\begin{array}{l} \mathfrak{A}\mu'' \equiv \quad\;\; \mathfrak{A}a'\xi'\zeta \;\;\equiv \mathfrak{A}^2a'\delta\zeta \\ a'\mu' \equiv - a'a''\xi''\zeta \equiv \mathfrak{A}^2a'\delta\zeta \end{array}\right\} \text{ d. i. } \mathfrak{A}\mu'' \equiv a'\mu'$$

und ebenso

$$\left.\begin{array}{l} \mathfrak{A}\nu'' \equiv - \mathfrak{A}a'\xi'\eta \;\;\equiv - \mathfrak{A}^2a'\delta\eta \\ a'\nu' \equiv \quad\;\; a'a''\xi''\eta \equiv - \mathfrak{A}^2a'\delta\eta \end{array}\right\} \text{ d. i. } \mathfrak{A}\nu'' \equiv a'\nu'$$

und somit die Richtigkeit der Congruenz (20). Da in gleicher Weise sich die beiden anderen der Congruenzen (7) als erfüllt zeigen, so haben wir eine Lösung der Gleichung (1) nachgewiesen, welche den Congruenzen (7) genügt.

Sollten die Elemente $\alpha, \alpha', \alpha''$ dieser Auflösung aber noch einen von 1 verschiedenen grössten gemeinsamen Theiler d haben, so könnte dieser nur ein Theiler von D sein, da der Modulus der Gleichungen (19) gleich D ist. Dann lehren aber diese Gleichungen, da die Grössen

$$\mu'\nu'' - \mu''\nu' = a\xi, \quad \mu''\nu - \mu\nu'' = a'\xi', \quad \mu\nu' - \mu'\nu = a''\xi''$$

keinen gemeinsamen Theiler besitzen, dass ϱ' und ϱ'' den Theiler d mit D gemeinsam haben müssten. Indessen darf man vor-

aussetzen, dass in der Substitution (17) die Grössen ϱ' und ϱ'' keinen gemeinsamen Theiler mit D haben.

In der That, wenn man diese Substitution mit der anderen:

$$\begin{aligned} z &= p^2\zeta + 2pq\zeta' + q^2\zeta'' \\ z' &= pr\zeta + (ps + qr)\zeta' + qs\zeta'' \\ z'' &= r^2\zeta + 2rs\zeta' + s^2\zeta'' \end{aligned}$$

zusammensetzt, in welcher p, q, r, s irgend welche vier ganze, der Gleichung

$$ps - qr = 1$$

genügende Zahlen sind, eine Substitution, durch welche (nach nr. 7 des ersten Capitels) die Form $zz'' - z'^2$ in sich selbst übergeführt wird, so wird die zusammengesetzte Substitution ebenso gut wie die Substitution (17) selbst, die Form G in

$$4(zz'' - z'^2)$$

verwandeln und also bei der vorigen Betrachtung statt ihrer zur Gewinnung der $\alpha, \alpha', \alpha''$ gewählt werden dürfen. In ihr treten aber an Stelle der Elemente ϱ' und ϱ'' die Ausdrücke

$$\begin{aligned} r' &= \varrho'p^2 + 2\sigma'pr + 2\tau'r^2 \\ r'' &= \varrho''p^2 + 2\sigma''pr + 2\tau''r^2. \end{aligned}$$

Ist nun ϖ irgend einer der ungeraden Primfaktoren, aus denen sich D zusammensetzt, und zugleich auch in ϱ' und ϱ'' enthalten, so ist wenigstens eine der Zahlen τ', τ'' nicht theilbar durch ϖ, und daher wird wenigstens eine der Zahlen r', r'' nicht theilbar durch ϖ, wenn man p theilbar, r nicht theilbar durch ϖ wählt. Ist aber ϖ einer der ungeraden Primfaktoren von D, die nicht gleichzeitig in beiden Zahlen ϱ' und ϱ'' aufgehen, so wird wenigstens eine der Zahlen r' und r'' durch ϖ nicht theilbar, sobald man r theilbar, p aber nicht theilbar durch ϖ wählt. Endlich wird wenigstens eine der Zahlen r', r'' ungerade sein, wenn man p ungerade wählt. Und da diese verschiedenen Congruenzbedingungen für p, r mit einander verträglich sind, wird man schliesslich p, r so wählen können, dass r' und r'' keinen gemeinsamen Theiler mit D haben können. Auch darf man hierbei offenbar jeden etwaigen

gemeinsamen Theiler der Zahlen p, r unterdrücken, d. h. sie relativ prim und also mit der Bedingungsgleichung

$$ps - qr = 1$$

verträglich voraussetzen. Auf solche Weise zeigt sich demnach, dass, wenn in der Substitution (17) die Elemente ϱ', ϱ'' mit D einen gemeinsamen Theiler hätten, diese Substitution für obiges Räsonnement durch eine andere ersetzt werden könnte, bei welcher die entsprechenden Elemente keinen solchen Theiler besässen; mit anderen Worten: man darf von vornherein voraussetzen, dass in der Substitution, welche zu den Werthen $\alpha, \alpha', \alpha''$ führt, ϱ', ϱ'' ohne gemeinsamen Theiler mit D sind. Daraus geht dann aber nach dem oben Gesagten hervor, dass auch $\alpha, \alpha', \alpha''$ keinen gemeinsamen Theiler besitzen, vielmehr eine eigentliche Auflösung der Gleichung (1) darstellen.

Auf solche Weise ist schliesslich gezeigt, was gezeigt werden sollte: Sind die Congruenzen (8) auflösbar, so giebt es zu jeder ihrer Wurzelcombinationen $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ eine eigentliche Auflösung der Gleichung (1), welche den Congruenzen (7) genügt.

4. Nachdem wir im Vorigen die Bedingungen kennen gelernt, unter denen die Gleichung (1) Auflösungen zulässt, wird es nun darauf ankommen, sie sämmtlich zu finden. Eine derselben ergiebt sich durch die Methode, mittels deren der letzte Satz bewiesen wurde, unmittelbar, aus dieser einen lassen aber alle übrigen sich herleiten. Diese Bemerkung hat bereits Gauss gemacht*) und dann gezeigt, dass sämmtliche Auflösungen der Gleichung (1) in folgender Gestalt gegeben werden können:

$$x = \frac{1}{t}\varphi(p, q), \quad x' = \frac{1}{t}\varphi'(p, q), \quad x'' = \frac{1}{t}\varphi''(p, q);$$

$\varphi, \varphi', \varphi''$ bezeichnen drei binäre quadratische Formen mit den beiden Unbestimmten p, q, und, um sämmtliche eigentliche Auflösungen zu finden, müssen diesen letzteren alle relativ primen Werthe gegeben, dann aber die Werthe der quadra-

*) Disquisitiones Arithm. art. 299 III.

tischen Formen $\varphi, \varphi', \varphi''$ durch ihren grössten gemeinsamen Theiler t dividirt werden. Nicht mit Unrecht hat G. Cantor*) darauf hingewiesen, wie diese Gauss'sche Lösung der Aufgabe insofern nicht ganz genügen könne, als sie nicht angebe, wie allgemein diese Zahl t mit den Zahlen p, q verbunden ist, sodass sie nur für jedes gegebene Paar dieser Zahlen durch eine besondere Rechnung gefunden werden kann; und er hat deshalb eine andere Form der Lösung gesucht. Nach ihm hat Dedekind**) eine Lösung derselben Aufgabe gegeben, welche sich vortheilhaft vor der seinen durch grosse Einfachheit auszeichnet. Wir wollen hier diese Dedekind'sche Lösung zur Darstellung bringen, wollen jedoch dabei, um der Form der Gauss'schen Auflösung, sowie dem schönen Cantor'schen Grundgedanken, der unmittelbar aus ihr entsprungen ist, möglichst Rechnung zu tragen, den Zusammenhang wahren, in welchem sie mit jenem steht, und aus der so gefundenen Auflösung dann auf einfache Weise die Cantor'schen Resultate erschliessen.

Die Betrachtungen der vorigen nr. haben gezeigt, in wie naher Beziehung die Auflösung der Gleichung (1) zu den Transformationen steht, welche die Form

$$f = ax^2 + a'x'^2 + a''x''^2$$

in die Form

$$4D(zz'' - z'^2)$$

verwandeln. Betrachten wir diese zunächst etwas näher. Sei eine solche wieder, wie in nr. 6 des ersten Capitels, bezeichnet mit:

$$(21)\qquad \begin{cases} x = \alpha_0{}^0 z + 2\alpha_0{}' z' + \alpha_0{}'' z'' \\ x' = \alpha_1{}^0 z + 2\alpha_1{}' z' + \alpha_1{}'' z'' \\ x'' = \alpha_2{}^0 z + 2\alpha_2{}' z' + \alpha_2{}'' z''; \end{cases}$$

alsdann werden folgende Gleichungen als charakteristisch für dieselbe bestehen:

*) In der Einleitung zu seiner früher genannten Inauguraldissertation.

**) Vorlesungen über Zahlentheorie von Dirichlet, 4. Auflage, S. 418 u. ff.

$$(22)\quad \begin{cases} 0 = a\alpha_0^{0\,2} + a'\alpha_1^{0\,2} + a''\alpha_2^{0\,2} \\ -D = a\alpha_0'^2 + a'\alpha_1'^2 + a''\alpha_2'^2 \\ 0 = a\alpha_0''^2 + a'\alpha_1''^2 + a''\alpha_2''^2 \\ 0 = a\alpha_0^0\alpha_0' + a'\alpha_1^0\alpha_1' + a''\alpha_2^0\alpha_2' \\ 2D = a\alpha_0^0\alpha_0'' + a'\alpha_1^0\alpha_1'' + a''\alpha_2^0\alpha_2'' \\ 0 = a\alpha_0'\alpha_0'' + a'\alpha_1'\alpha_1'' + a''\alpha_2'\alpha_2''. \end{cases}$$

Ferner bestehen den dortigen Gleichungen (42) und (44) gemäss die Beziehungen:

$$(23)\quad \begin{cases} 2Dz = \alpha_0'' \cdot ax + \alpha_1'' \cdot a'x' + \alpha_2'' \cdot a''x'' \\ 2Dz' = -(\alpha_0' \cdot ax + \alpha_1' \cdot a'x' + \alpha_2' \cdot a''x'') \\ 2Dz'' = \alpha_0^0 \cdot ax + \alpha_1^0 \cdot a'x' + \alpha_2^0 \cdot a''x'' \end{cases}$$

und

$$(24)\quad \begin{cases} a'a'' = \alpha_0^0\alpha_0'' - \alpha_0'^2 \\ a''a = \alpha_1^0\alpha_1'' - \alpha_1'^2 \\ aa' = \alpha_2^0\alpha_2'' - \alpha_2'^2 \\ 0 = \alpha_1^0\alpha_2'' + \alpha_2^0\alpha_1'' - 2\alpha_1'\alpha_2' \\ 0 = \alpha_2^0\alpha_0'' + \alpha_0^0\alpha_2'' - 2\alpha_0'\alpha_2' \\ 0 = \alpha_0^0\alpha_1'' + \alpha_1^0\alpha_0'' - 2\alpha_0'\alpha_1'. \end{cases}$$

Die ersten drei der letzteren Gleichungen lassen erkennen, dass, wenn man unter (21) irgend eine ganzzahlige Transformation der Form f in die Form

$$4D(zz'' - z'^2)$$

versteht, $\alpha_0', \alpha_1', \alpha_2'$ ganze Zahlen, die Coefficienten von z' in der Substitution also gerade Zahlen sein müssen.

Denkt man sich nun andererseits die drei quadratischen Formen

$$(25)\quad \begin{cases} \varphi = \alpha_0^0 p^2 + 2\alpha_0' pq + \alpha_0'' q^2 \\ \varphi' = \alpha_1^0 p^2 + 2\alpha_1' pq + \alpha_1'' q^2 \\ \varphi'' = \alpha_2^0 p^2 + 2\alpha_2' pq + \alpha_2'' q^2 \end{cases}$$

und fragt nach den Bedingungen, denen die Coefficienten genügen müssen, wenn diese Formen, an Stelle von x, x', x'' eingesetzt, die Gleichung (1) befriedigen sollen, welche Werthe p, q auch bedeuten, so finden sich unmittelbar folgende Gleichungen:

$$\begin{aligned}
0 &= a\alpha_0^{0\,2} + a'\alpha_1^{0\,2} + a''\alpha_2^{0\,2} \\
0 &= a\alpha_0''^2 + a'\alpha_1''^2 + a''\alpha_2''^2 \\
0 &= a\alpha_0^0\alpha_0' + a'\alpha_1^0\alpha_1' + a''\alpha_2^0\alpha_2' \\
0 &= a\alpha_0'\alpha_0'' + a'\alpha_1'\alpha_1'' + a''\alpha_2'\alpha_2'' \\
0 &= 4(a\alpha_0'^2 + a'\alpha_1'^2 + a''\alpha_2'^2) \\
&\quad + 2(a\alpha_0^0\alpha_0'' + a'\alpha_1^0\alpha_1'' + a''\alpha_2^0\alpha_2''),
\end{aligned}$$

von welchen, wie man sieht, die vier ersten mit vier von den Gleichungen (22) identisch sind, während die letzte durch die folgenden zwei ersetzt werden kann:

$$\begin{aligned}
-K &= 2(a\alpha_0'^2 + a'\alpha_1'^2 + a''\alpha_2'^2) \\
K &= a\alpha_0^0\alpha_0'' + a'\alpha_1^0\alpha_1'' + a''\alpha_2^0\alpha_2'',
\end{aligned}$$

die mit den übrigen Gleichungen (22) identisch werden, sobald man für K den Werth $2D$ wählt. Alsdann ist aber die aus den Coefficienten der Formen (25) gebildete Substitution (21) eine Transformation von f in

$$4D(zz'' - z'^2).$$

Hinfort sollen die so gebildeten quadratischen Formen (25) eine Formallösung der Gleichung (1) genannt werden.

Man sieht: jede Formallösung der Gleichung (1) führt zu einer Transformation von f in $4D(zz'' - z'^2)$ und umgekehrt.

5. Nimmt man nun an, man habe eine eigentliche Auflösung der Gleichung (1) bereits gefunden:

$$x = \alpha_0^0, \quad x' = \alpha_1^0, \quad x'' = \alpha_2^0,$$

sodass

$$a\alpha_0^{0\,2} + a'\alpha_1^{0\,2} + a''\alpha_2^{0\,2} = 0 \tag{26}$$

ist, so lässt sich daraus sogleich eine Transformation der Form f in $4D(zz'' - z'^2)$ herleiten. Da die drei Zahlen $a\alpha_0^0$, $a'\alpha_1^0$, $a''\alpha_2^0$ zu je zweien prim sind, muss dieser Gleichung zufolge eine von ihnen, etwa $a\alpha_0^0$, gerade, die beiden anderen ungerade sein, und weil deshalb auch $2a\alpha_0^0$, $a'\alpha_1^0$, $a''\alpha_2^0$ relativ prim sind, so kann man der Gleichung

$$a\alpha_0^0 l + a'\alpha_1^0 l' + a''\alpha_2^0 l'' = 1 \tag{27}$$

durch ganze Zahlen l, l', l'' Genüge leisten, von denen die erste gerade ist.

Setzt man dann

(28) $$al^2 + a'l'^2 + a''l''^2 = h$$

und

$$\alpha_0'' = (2l - h\alpha_0^0)D, \quad \alpha_1'' = (2l' - h\alpha_1^0)D, \quad \alpha_2'' = (2l'' - h\alpha_2^0)D,$$

so finden sich sogleich die Beziehungen

(29) $$a\alpha_0^0\alpha_0'' + a'\alpha_1^0\alpha_1'' + a''\alpha_2^0\alpha_2'' = 2D$$

sowie

(30) $$a\alpha_0''^2 + a'\alpha_1''^2 + a''\alpha_2''^2 = 0.$$

Offenbar wird man von den noch übrigen der Gleichungen (22) der 4ten und 6ten Genüge leisten, wenn man $\alpha_0', \alpha_1', \alpha_2'$ durch die folgenden Gleichungen bestimmt:

(31) $$\begin{cases} 2D\alpha_0' = -a'a''(\alpha_1^0\alpha_2'' - \alpha_2^0\alpha_1'') \\ 2D\alpha_1' = -a''a(\alpha_2^0\alpha_0'' - \alpha_0^0\alpha_2'') \\ 2D\alpha_2' = -aa'(\alpha_0^0\alpha_1'' - \alpha_1^0\alpha_0''), \end{cases}$$

wodurch sie als ganze Zahlen bestimmt werden, da diese Gleichungen mit den anderen:

$$\begin{aligned} \alpha_0' &= -a'a''(l''\alpha_1^0 - l'\alpha_2^0) \\ \alpha_1' &= -a''a(l\alpha_2^0 - l''\alpha_0^0) \\ \alpha_2' &= -aa'(l'\alpha_0^0 - l\alpha_1^0) \end{aligned}$$

gleichbedeutend sind. Für diese Werthe von $\alpha_0', \alpha_1', \alpha_2'$ wird jedoch endlich

$$\begin{aligned} &a\alpha_0'^2 + a'\alpha_1'^2 + a''\alpha_2'^2 \\ &= D[a'a''(l''\alpha_1^0 - l'\alpha_2^0)^2 + a''a(l\alpha_2^0 - l''\alpha_0^0)^2 \\ &\qquad + aa'(l'\alpha_0^0 - l\alpha_1^0)^2] \\ &= D[(al^2 + a'l'^2 + a''l''^2)(a\alpha_0^{02} + a'\alpha_1^{02} + a''\alpha_2^{02}) \\ &\qquad - (al\alpha_0^0 + a'l'\alpha_1^0 + a''l''\alpha_2^0)^2], \end{aligned}$$

was mit Rücksicht auf die Gleichungen (26) und (27) in

$$a\alpha_0'^2 + a'\alpha_1'^2 + a''\alpha_2'^2 = -D$$

übergeht, sodass die zweite der Gleichungen (22), und, wie aus den erhaltenen Formeln sogleich ersichtlich, diese sämmtlichen Gleichungen erfüllt sind. Die so bestimmten Zahlen α bilden mithin eine ganzzahlige Transformation (21) der Form f in die Form $4D(zz'' - z'^2)$, sodass vermöge der Gleichungen (21) oder ihrer Umkehrung (23) die Gleichung

(32) $$ax^2 + a'x'^2 + a''x''^2 = 4D(zz'' - z'^2)$$

identisch erfüllt wird. Setzt man nun zur Vereinfachung

$$\begin{array}{lll} \alpha_0^0 = u, & \alpha_1^0 = u', & \alpha_2^0 = u'' \\ 2l - h\alpha_0^0 = w, & 2l' - h\alpha_1^0 = w', & 2l'' - h\alpha_2^0 = w'' \\ l''\alpha_1^0 - l'\alpha_2^0 = v, & l\alpha_2^0 - l''\alpha_0^0 = v', & l'\alpha_0^0 - l\alpha_1^0 = v'', \end{array}$$

Bestimmungen, aus welchen sich, da zufolge (27) h ungerade sein muss, sogleich die Congruenzen

(33) $$w \equiv u, \quad w' \equiv u', \quad w'' \equiv u'' \pmod{2}$$

ergeben, so nehmen die Substitutionen (21) und (23) die Form:

$$\begin{aligned} x &= uz - 2a'a''vz' + Dwz'' \\ x' &= u'z - 2a''av'z' + Dw'z'' \\ x'' &= u''z - 2aa'v''z' + Dw''z'' \end{aligned}$$

resp. die Form:

$$\begin{aligned} 2Dz &= Dw \cdot ax + Dw' \cdot a'x' + Dw'' \cdot a''x'' \\ 2Dz' &= a'a''v \cdot ax + a''av' \cdot a'x' + aa'v'' \cdot a''x'' \\ 2Dz'' &= u \cdot ax + u' \cdot a'x' + u'' \cdot a''x'' \end{aligned}$$

an, und der Umstand, dass vermöge ihrer die Gleichung (32) erfüllt wird, lässt sich, wie unmittelbar zu übersehen, auch so ausdrücken, dass vermöge jedes der folgenden beiden Systeme von Gleichungen:

(34) $$\begin{cases} 2x = uz - 2a'a''vz' + wz'' \\ 2x' = u'z - 2a''av'z' + w'z'' \\ 2x'' = u''z - 2aa'v''z' + w''z'' \end{cases}$$

und

(35) $$\begin{cases} z = w \cdot ax + w' \cdot a'x' + w'' \cdot a''x'' \\ z' = v \cdot x + v' \cdot x' + v'' \cdot x'' \\ z'' = u \cdot ax + u' \cdot a'x' + u'' \cdot a''x'' \end{cases}$$

die Gleichung

(36) $$ax^2 + a'x'^2 + a''x''^2 = zz'' - Dz'^2$$

identisch erfüllt wird. Nun entsprechen ersichtlich nach den Gleichungen (35) ganzzahligen Systemen x, x', x'' auch ganzzahlige Systeme z, z', z'', und zwar, wie aus den Congruenzen

(33) sogleich sich ergiebt, solche ganzzahlige Systeme, für welche

(37) $$z \equiv z'' \pmod{2}$$

ist; aber nach den Gleichungen (34) werden auch umgekehrt solchen ganzzahligen Systemen z, z', z'', welche die Bedingung (37) erfüllen, ganzzahlige Systeme x, x', x'' zugeordnet sein, und sonach erschliesst man aus dem Vorigen den Dedekind'schen Satz:

Man erhält sämmtliche ganzzahligen Lösungen der Gleichung

(1) $$ax^2 + a'x'^2 + a''x''^2 = 0,$$

wenn man in den Gleichungen (34) für z, z', z'' sämmtliche ganzzahligen Systeme setzt, welche zugleich der Gleichung

(38) $$zz'' = Dz'^2$$

und der Congruenz

$$z \equiv z'' \pmod{2}$$

Genüge leisten. Damit aber x, x', x'' eine *eigentliche* Lösung bilden, ist zudem nothwendig, doch auch hinreichend, dass z und z'' keinen ungeraden gemeinsamen Theiler haben und, wenn sie beide gerade sind, die Congruenz

(39) $$z + z'' \equiv 2 \pmod{4}$$

erfüllen.

Der letztere Zusatz ist noch zu beweisen. — Das behauptete Verhalten der Zahlen z, z'' ist erstens nothwendig. Denn, hätten z, z'' einen gemeinsamen ungeraden Primtheiler, so würde dieser wegen (38), da D keinen quadratischen Theiler hat, auch in z' und folglich nach (34) in allen drei Zahlen x, x', x'' aufgehen; wären z und z'' und deshalb wegen (38) auch z' gerade, die Congruenz (39) aber nicht erfüllt, also

$$z \equiv z'' \pmod{4},$$

so erhielte man aus (34)

$$\left.\begin{aligned} 2x &\equiv (u + w)z \equiv 0 \\ 2x' &\equiv (u' + w')z' \equiv 0 \\ 2x'' &\equiv (u'' + w'')z'' \equiv 0 \end{aligned}\right\} \pmod{4}$$

also wären x, x', x'' sämmtlich gerade. In beiden Fällen würde daher die Lösung x, x', x'' keine eigentliche sein. — Die behauptete Beschaffenheit von z und z'' ist aber zweitens auch hinreichend. Denn jeder gemeinsame ungerade Theiler von x, x', x'' ginge nach (35) auch in z und z'' auf; hätten sie aber den gemeinsamen Theiler 2, so wären nach (35) z und z'' gerade, zugleich aber

$$z + z'' \equiv 0 \pmod{4},$$

die Lösung x, x', x'' muss also eine eigentliche sein, sobald z und z'' die angegebenen Bedingungen erfüllen.

6. Aus dieser Dedekind'schen Lösung der Aufgabe, alle (eigentlichen) Lösungen der Gleichung (1) aus einer von ihnen herzuleiten, lässt sich — wenigstens im Wesentlichen — sehr leicht auch diejenige Lösung gewinnen, welche G. Cantor dafür gegeben hat. Die allgemeinste Art, der Gleichung (38) zu genügen, ist offenbar durch die Gleichungen

$$(40) \qquad z = d\delta p^2, \quad z' = \delta pq, \quad z'' = d''\delta q^2$$

geliefert, wenn dd'' irgend eine Zerlegung von D in zwei positive Faktoren, δ, p, q aber irgend welche ganze Zahlen vorstellen. In Folge dieser Werthe von z, z', z'' nehmen die Gleichungen (34) die Gestalt an:

$$x = \frac{\delta}{2} \cdot \psi, \quad x' = \frac{\delta}{2} \cdot \psi', \quad x'' = \frac{\delta}{2} \cdot \psi'',$$

wenn unter ψ, ψ', ψ'' die folgenden drei quadratischen Formen:

$$\begin{aligned} \psi \ &= ud \cdot p^2 - 2a'a''v \cdot pq + wd'' \cdot q^2 \\ \psi' &= u'd \cdot p^2 - 2a''av' \cdot pq + w'd'' \cdot q^2 \\ \psi'' &= u''d \cdot p^2 - 2aa'v'' \cdot pq + w''d'' \cdot q^2 \end{aligned}$$

verstanden werden, oder auch die folgende:

$$(41) \qquad x = \frac{\delta}{2d} \cdot \varphi, \quad x' = \frac{\delta}{2d} \cdot \varphi', \quad x'' = \frac{\delta}{2d} \cdot \varphi'',$$

wenn man setzt:

$$(42) \qquad \begin{cases} \varphi \ = \alpha_0{}^0 \cdot (dp)^2 + 2\alpha_0{}' \cdot (dp)q + \alpha_0{}'' \cdot q^2 \\ \varphi' = \alpha_1{}^0 \cdot (dp)^2 + 2\alpha_1{}' \cdot (dp)q + \alpha_1{}'' \cdot q^2 \\ \varphi'' = \alpha_2{}^0 \cdot (dp)^2 + 2\alpha_2{}' \cdot (dp)q + \alpha_2{}'' \cdot q^2. \end{cases}$$

Damit aber die Formeln (41) die eigentlichen Auf-

lösungen der Gleichung (1) liefern, sind nun die Zahlen d, d'', δ, p, q solcher Beschränkung zu unterwerfen, dass z und z'' die oben angegebenen Bedingungen erfüllen. Damit z', z'' ohne gemeinsamen ungeraden Theiler werden, ist nothwendig, dass δ nur eine Potenz von 2 ist, welche der Congruenz (39) wegen nicht höher als die erste sein darf; also ist $\delta = \pm 1$ oder $\delta = \pm 2$ zu wählen. Ferner dürfen auch p, q keinen gemeinsamen ungeraden Theiler haben, sie dürfen aber auch nicht beide gerade sein, weil sonst

$$z \equiv z'' \equiv 0 \pmod{4}$$

sein würde, gegen (39); also müssen p, q als relative Primzahlen gewählt werden. Zudem muss endlich p auch ohne gemeinsamen ungeraden Theiler mit d'', q ohne einen solchen mit d angenommen werden. Im Weiteren unterscheidet man zweckmässig die beiden Fälle eines ungeraden und eines geraden D.

Sei erstens $D = aa'a''$ ungerade. Dann muss

$$\delta = \pm 1$$

gesetzt werden, wenn p, q als ungerade relative Primzahlen gewählt werden, da für $\delta = \pm 2$ die Bedingung (39) nicht erfüllt werden könnte. Wird aber eine der Zahlen p, q gerade, die andere ungerade gewählt, so muss $\delta = \pm 2$ genommen werden, da sonst die Congruenz (37) nicht stattfände.

Ist zweitens $D = aa'a''$ gerade, so wird einer der Faktoren d, d'' gerade, der andere ungerade, und der gerade Faktor congruent 2 (mod. 4) sein, da D keine quadratischen Theiler enthält. Wenn dann p, q zunächst ungerade genommen werden, so ist wegen (37) $\delta = \pm 2$ zu setzen, wo dann auch (39) erfüllt ist. Wählt man aber eine der Zahlen p, q gerade, die andere ungerade, so hat man zu setzen

$\delta = \pm 2$, wenn d, p gerade, also d'', q ungerade,
oder d'', q gerade, also d, p ungerade,
$\delta = \pm 1$, wenn d, q gerade, also d'', p ungerade,
oder d'', p gerade, also d, q ungerade

sind. Die Beschränkungen, welche für die Zahlen δ, p, q nothwendig und hinreichend sind, stellen sich demnach in folgender Uebersicht dar:

Ist I) D ungerade und $d \cdot d''$ irgend eine Zerfällung von D, so muss

entweder $\delta = \pm 1$, p prim zu $2d''$, q prim zu $2d$
oder $\delta = \pm 2$, p gerade und prim zu d'', q prim zu $2d$ oder p prim zu $2d''$, q gerade und prim zu d sein.

Ist II) D gerade gleich $2P$ und $\pi \cdot \pi''$ irgend eine Zerfällung von P, so muss

wenn a) $d = 2\pi$, $d'' = \pi''$ ist,
entweder $\delta = \pm 1$, p prim zu $2\pi''$, q prim zu π und gerade
oder $\delta = \pm 2$, p prim zu π'', q prim zu 2π,
wenn dagegen b) $d = \pi$, $d'' = 2\pi''$ ist,
entweder $\delta = \pm 1$, p gerade und prim zu π'', q prim zu 2π
oder $\delta = \pm 2$, p prim zu $2\pi''$, q prim zu π sein.

Man überzeugt sich aber unschwer, dass der zweite Fall IIa unter dem ersten Falle IIb, sowie der zweite Fall IIb unter dem ersten Falle IIa enthalten also von der Betrachtung auszuschliessen ist. Ausserdem müssen in allen Fällen die Zahlen p, q unter einander prim angenommen werden. Mit Beachtung dieser näheren Bestimmungen ergeben die Formeln (41) sämmtliche eigentliche Auflösungen der Gleichung (1) und solche ausschliesslich. Man bemerke aber ferner, dass nach Ausschluss der genannten beiden Fälle die Formeln (40) für jedes bestimmte System z, z', z'' auch nur ein System d, d'', δ, p, q ergeben, wenn man zwei Systeme p, q und $-p$, $-q$ immer nur als ein einziges rechnet, dass also dann verschiedenen Systemen d, d'', δ, p, q auch verschiedene Systeme z, z', z'' und folglich nach den Gleichungen (34) und (35) auch verschiedene Systeme x, x', x'' von Lösungen der Gleichung (1) zugehören. In Folge davon werden dann die Formeln (41) auch nur jede Lösung einmal liefern.

Diese Formeln repräsentiren nun offenbar eine gewisse Anzahl von Formallösungen der Gleichung (1), eine Anzahl, welche leicht angebbar, nämlich ersichtlich gleich der Anzahl der zulässigen Werthcombinationen der drei Zahlen d, d'', δ ist. Nennt man wieder θ die Anzahl der ver-

schiedenen ungeraden Primfaktoren, aus denen D besteht, so ist diese Anzahl (nach Ausschluss der genannten beiden Fälle unter II) für eine ungerade wie gerade Determinante D gleich $2^{\varrho+2}$. In jeder einzelnen jener Formallösungen sind aber, dem Gesagten entsprechend, die Zahlen p, q auf eine Anzahl bestimmter arithmetischer Reihen beschränkt. In der That ergeben die obigen Bestimmungen für diese Zahlen, dass sie (mod. $2D$) einer Anzahl von Congruenzpaaren:

$$(43) \qquad p \equiv p_0, \; q \equiv q_0 \pmod{2D}$$

zu genügen haben, welche, jenachdem δD ungerade oder gerade ist, resp. gleich $D \cdot \varphi(D)$ oder $2D \cdot \varphi(D)$ gefunden wird.

Und somit gelangen wir schliesslich zu folgendem Resultate:

Sämmtliche eigentliche Lösungen der Gleichung (1) werden mittels einer endlichen Anzahl von Formallösungen durch die Formeln (41) und jede nur einmal geliefert, wenn in denselben die unbestimmten ganzen Zahlen p, q als relative Primzahlen aus einer endlichen Anzahl von Paaren arithmetischer Reihen ausgewählt werden, welche für jede der Formallösungen durch zugehörige Congruenzen von der Form (43) definirt sind.

Die hier gegebenen Sätze sind im wesentlichen mit den Hauptresultaten der oben angeführten Cantor'schen Arbeit übereinstimmend (vgl. die §§ 9 und 11 derselben).

7. Die im Vorigen entwickelte Theorie der Gleichung

$$(1) \qquad ax^2 + a'x'^2 + a''x''^2 = 0$$

ist nicht nur an sich von hoher Bedeutung, sondern bietet auch ein historisches Interesse, insofern die Bedingungen ihrer Auflösbarkeit die Grundlage ausmachen für den ersten Beweis, der für das quadratische Reciprocitätsgesetz gegeben worden ist. In der That beruht der erste Beweis desselben, welchen Legendre versucht hat*), abgesehen von

*) S. Legendre in der hist. de l'Acad. des Sciences de Paris 1785

einigen einfachen Sätzen, zu welchen die Pell'sche Gleichung führt und welche auch von uns im fünften Capitel zum Beweise des Reciprocitätsgesetzes benutzt worden sind, wesentlich auf jenen Bedingungen. Viel später erst ist von Kummer gezeigt worden*), wie man bei solchem Beweise die Gleichung (1) gänzlich vermeiden und allein mit der Pell'schen Gleichung auskommen kann. Beide Beweise setzen übrigens, wie bezüglich des Legendre'schen von Gauss hervorgehoben worden ist, voraus, dass zu jeder Primzahl von der Form $4n + 1$ eine Primzahl von der Form $4n + 3$ gefunden werden könne, von welcher jene quadratischer Nichtrest ist, eine Voraussetzung, deren Richtigkeit schwerlich ohne Hilfe des zu beweisenden Reciprocitätsgesetzes wird zu bestätigen sein.

Ungleich wichtiger ist der Umstand, auf welchen zuerst Arndt**) aufmerksam gemacht hat, dass sich auf die Gleichung (1) auch ein Beweis des Gauss'schen Satzes von der Duplikation der Classen gründen lässt, dieses wichtigen Satzes, der in nr. 5 des fünften Capitels aus ganz anderer Quelle hergeleitet worden ist. Da die Hilfsmittel, deren wir uns bedient haben, die Theorie der Gleichung (1) zu begründen, wesentlich elementarere Sätze aus der Lehre von den ternären Formen sind, als diejenigen, auf denen jener frühere Beweis des Gauss'schen Satzes beruhte, so ist die Arndt'sche Herleitung desselben als die einfachere zu betrachten und die Aussage nicht ungerechtfertigt, dass jener berühmte Satz von der Duplikation der Classen im Grunde auf die Bedingungen der Auflösbarkeit der Gleichung (1) zurückkomme.

Der in nr. 3 hergeleitete Satz verstattet seine Ausdehnung auch auf den Fall, wo die Coefficienten a, a', a'' quadratische

---

oder in der théorie des nombres, II partie § 6: théorème contenant une loi de réciprocité, qui existe entre deux nombres premiers quelconques.

*) Kummer, zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist; in den Abhh. der Berliner Akad. 1861, sowie auch in Borch. J. f. d. r. u. a. Math. 100 S. 10.

**) In Borch. J. f. Math. 56 S. 73: über die Anzahl der Genera der quadratischen Formen.

Theiler haben*), und erlaubt dann, den Gauss'schen Satz sogleich in voller Allgemeinheit zu beweisen**). Beschränkt man sich aber zunächst auf den Fall, in welchem die Determinante D der binären quadratischen Formen von quadratischen Faktoren frei ist, so braucht man garnicht den vollständigen angezogenen Hilfssatz, sondern nur den Theil desselben, welcher aussagt, dass die Gleichung (1) eine eigentliche Lösung hat, sobald die Congruenzen (8) erfüllt sind.

Wenn dann nämlich (A, B, C) irgend eine Form des Hauptgeschlechtes für die Determinante D ist, so darf man voraussetzen, dass A eine ungerade und gegen D prime Zahl ist, die auch als positiv gedacht werden darf, wenn im Falle negativer Determinanten nur positive Formen betrachtet werden. Da A quadratische Faktoren haben kann, setze man $A = ap^2$, wo nun a von quadratischen Faktoren frei sein soll. Nach der Gleichung

$$B^2 - ap^2 \cdot C = D$$

ist die Zahl D quadratischer Rest von a. Da andererseits die Form (ap^2, B, C) dem Hauptgeschlechte angehören soll, so sind die quadratischen Charaktere von ap^2 also auch von a mit Bezug auf jeden ungeraden Primfaktor von D gleich $+1$, also ist auch umgekehrt a quadratischer Rest von D. Da endlich a und D relativ prim und nicht beide negativ sind, so ist nach der Theorie der Gleichung (1) die Gleichung

$$ax^2 + Dy^2 - z^2 = 0$$

in ganzen Zahlen x, y, z ohne gemeinsamen Theiler auflösbar d. h. die Zahl ax^2 ist eigentlich darstellbar durch die Hauptform $(1, 0, -D)$ von der Determinante D; auch ist sie prim gegen D, da, wenn ax^2 also x einen Primfaktor mit D gemeinsam hätte, dieser auch in z und, da D keine quadratischen Theiler hat, auch in y aufgehen müsste.

Ferner wird die zu D prime Zahl ap^2 eigentlich durch die Form (A, B, C) dargestellt, und folglich die zu D prime Quadratzahl $(apx)^2 = ap^2 \cdot ax^2$ durch die Formen derjenigen

*) S. Dedekind, Vorl. üb. Zahlentheorie von Dirichlet, 4. Aufl. S. 422 u. ff.

**) Ebendaselbst S. 432

Classe, welche aus der Hauptclasse und derjenigen der Form (A, B, C) zusammengesetzt ist, d. h. durch die Formen der Classe von (A, B, C).

Mithin giebt es eine Form dieser Classe

$$(h^2, \varkappa, l),$$

wo im ersten Coefficienten h den Absolutwerth von apx bedeutet. Wenn nun zuerst h ungerade ist, so ist die Form

$$(h, \varkappa, lh)$$

eigentlich primitiv, da ihre Determinante D ohne quadratische Theiler und h ungerade ist, und, falls $D < 0$, positiv, da $h > 0$ ist; die Form $(h^2, \varkappa, l)$ aber entsteht aus ihr durch Duplikation, wie es die Identität

$$(hX^2 + 2\varkappa XY + hlY^2)(hX'^2 + 2\varkappa X'Y' + hlY'^2) \\ = h^2X''^2 + 2\varkappa X''Y'' + lY''^2$$

erweist, in welcher

$$X'' = XX' - lYY', \quad Y'' = h(XY' + X'Y) + 2\varkappa YY'$$

gedacht ist. Ist dagegen h gerade, so folgt aus der Gleichung

$$\varkappa^2 - h^2 l = D,$$

weil D nicht durch 4 theilbar ist, dass $\varkappa$ ungerade sein muss, ebenso wie es l ist, da die Form $(h^2, \varkappa, l)$ zugleich mit (A, B, C) eigentlich-primitiv ist. Also wird auch die im Falle $D < 0$ positive Form

$$(2h, h + \varkappa, \lambda),$$

in welcher

$$\lambda = \frac{(h + \varkappa)^2 - D}{2h} = (l + 1)\frac{h}{2} + \varkappa$$

gedacht ist, eigentlich-primitiv. Aus dieser Form entsteht aber die Form $(h^2, \varkappa, l)$ durch Duplikation, wie aus der Identität

$$(2hX^2 + 2(h + \varkappa)XY + \lambda Y^2)(2hX'^2 + 2(h + \varkappa)X'Y' + \lambda Y'^2) \\ = h^2X''^2 + 2\varkappa X''Y'' + lY''^2$$

hervorgeht, in welcher unter X'', Y'' die Ausdrücke

$$X'' = 2XX' + XY' + X'Y + \frac{1 - l}{2}YY'$$

$$Y'' = h(XY' + X'Y + YY') + \varkappa YY'$$

verstanden werden. Somit entsteht die Classe, welcher (A, B, C) angehört, d. h. jede Classe des Hauptgeschlechtes durch Duplikation.

Durch das Vorstehende ist der ausgesprochene Satz nun zwar nur für Formen einer Determinante erwiesen, welche frei ist von quadratischen Faktoren. Doch genügt dieser Nachweis, um ihn auch für Formen jeder beliebigen Determinante zu begründen. In der That folgt aus dem Bewiesenen für die specielleren Determinanten D die Gleichheit $K(D) = Q(D)$ (s. fünftes Capitel) und somit auch die andere: $G(D) = \mathfrak{A}(D)$ d. i. nach der Gauss'schen Schlussweise (das. nr. 5) die Existenz eines Geschlechts für jeden der zulässigen Gesammtcharaktere. Hieraus lässt sich aber auf eine einfache Weise, wie Arndt in der angeführten Abhandlung gezeigt hat, die Existenz eines Geschlechts auch für jeden der zulässigen Gesammtcharaktere bei einer beliebigen Determinante also, nach der Gauss'schen Schlussweise, die Gleichung $G(D) = \mathfrak{A}(D)$ sowie die andere: $K(D) = Q(D)$ ableiten und somit allgemein der Satz begründen, dass jede Classe des Hauptgeschlechts für irgend eine Determinante durch Duplikation entsteht.

8. In unmittelbarstem Zusammenhange mit der hier entwickelten Auflösung der Gleichung (1) steht eine andere Aufgabe, die schon die Mathematiker vor Gauss beschäftigt hat*), die Auflösung der Gleichung

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0 \tag{44}$$

in rationalen Zahlen x, y. In der That, diese Aufgabe ist vollkommen identisch mit der andern: die Gleichung

$$ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + fz^2 = 0$$

in ganzen Zahlen x, y, z aufzulösen, eine Aufgabe, welche nach nr. 1 auf die Auflösung einer Gleichung von der Gestalt

---

*) Schon Euler hat die Aufgabe unter gewissen Voraussetzungen gelöst (Commentat. Petropolenses t. 6, 9 und 18), doch erst Lagrange (in hist. de l'Acad. de Berlin 1767 p. 165 und 1768 p. 181) gab ihre vollständige Lösung, die jedoch von der hier dargestellten Gauss'schen wesentlich verschieden ist. S. dazu auch Scheffler's Diss. inaug. in Crelle's J. f. Math. 45 S. 349.

der Gleichung (1) zurückkommt. Hat man nun die Gleichung (44) in rationalen Zahlen vollständig gelöst, so besitzt man damit zwar implicite auch ihre Auflösung in ganzen Zahlen, doch würde es einer Methode bedürfen, um diese ganzzahligen Auflösungen aus der Menge der rationalen, die meist unendlich gross ist, auszuscheiden. Statt dessen kann man geradezu verfahren, wie folgt.

Man hat, wie in der analytischen Geometrie, drei verschiedene Fälle zu unterscheiden, jenachdem der Ausdruck $b^2 - ac$ Null, negativ oder positiv ist. Sei 1) $b^2 - ac = 0$. Ist dann θ der grösste gemeinsame Theiler von a und c, so müssen a und c, weil ihr Produkt ein Quadrat ist, resp. gleich $\theta\alpha^2$ und $\theta\gamma^2$, also $b = \theta\alpha\gamma$ sein, und somit wird

$$ax^2 + 2bxy + cy^2 = \theta(\alpha x + \gamma y)^2.$$

Setzt man demnach

$$\alpha x + \gamma y = z, \tag{45}$$

so nimmt die Gleichung (44) die Gestalt an:

$$2dx + 2ey = -f - \theta z^2,$$

aus welcher, in Verbindung mit (45)

$$2(e\alpha - d\gamma) \cdot x = \quad 2ez + \gamma f + \gamma\theta z^2$$
$$2(e\alpha - d\gamma) \cdot y = -2dz - \alpha f - \alpha\theta z^2$$

also, wenn $e\alpha - d\gamma$ von Null verschieden ist,

$$x = \frac{2ez + \gamma f + \gamma\theta z^2}{2(e\alpha - d\gamma)}, \quad y = \frac{-2dz - \alpha f - \alpha\theta z^2}{2(e\alpha - d\gamma)} \tag{46}$$

hervorgeht, Formeln, welche die Gleichung (44) für jeden Werth von z erfüllen werden. Damit aber x, y ganzzahlig werden, darf man z wegen (45) nur ganzzahlige Werthe beilegen, für welche die letztgeschriebenen Ausdrücke gleichzeitig ganzzahlig werden. Um alle diese Werthe von z zu finden, wird es genügen, diejenigen zu ermitteln, welche positiv und kleiner als $2(e\alpha - d\gamma)$ sind, denn Werthe von z, welche nach diesem Modulus congruent sind, geben stets gleichzeitig für beide x und y ganzzahlige, oder gleichzeitig nicht für beide x, y ganzzahlige Werthe. Sind also

$$z_1, z_2, \ldots z_r$$

diejenigen Werthe von z, wenn überhaupt solche vorhanden sind, welche x und y ganzzahlig machen und zugleich positiv und kleiner als $2(e\alpha - d\gamma)$ sind, so liefern die Formeln (46) die sämmtlichen ganzzahligen Auflösungen der Gleichung (44), wenn man in ihnen setzt:

$$z \equiv z_1, \; z \equiv z_2, \; \cdots z \equiv z_r \pmod{2(e\alpha - d\gamma)}.$$

Ist aber $e\alpha = d\gamma$, so ergiebt sich, wenn h der grösste gemeinsame Theiler von e, d ist, mit Rücksicht darauf, dass α, γ relativ prim sind, $d = h\alpha$, $e = h\gamma$, die Gleichung (44) erhält die Gestalt

$$(\theta\alpha x + \theta\gamma y + h)^2 + f\theta - h^2 = 0$$

und wird keine ganzzahlige Auflösung haben, wenn $h^2 - f\theta$ keine positive Quadratzahl ist; ist aber $h^2 - f\theta$ eine solche: $\varkappa^2$, so löst man die vorige Gleichung, indem man

$$\text{entweder } \theta\alpha x + \theta\gamma y = \varkappa - h$$
$$\text{oder } \theta\alpha x + \theta\gamma y = -(\varkappa + h)$$

setzt; die Gleichung (44) wird also keine ganzzahligen Auflösungen haben, wenn weder $\varkappa - h$ noch $\varkappa + h$ durch θ theilbar ist, im entgegengesetzten Falle die unendlich vielen Auflösungen x, y der einen oder der anderen dieser Gleichungen oder beider.

Sei jetzt $b^2 - ac$ von Null verschieden. Dann entferne man, wie in der analytischen Geometrie der Kegelschnitte zunächst die Glieder erster Dimension aus der Gleichung (44) vermittelst der Substitution

$$(47) \quad p = (b^2 - ac)x + be - cd, \; q = (b^2 - ac)y + bd - ae,$$

wodurch die Gleichung in die Gestalt

$$(48) \qquad ap^2 + 2bpq + cq^2 = M$$

übergeht, in welcher M ein ganzzahliger Werth ist; ganzzahligen x, y aber entsprechen gewiss ganzzahlige Lösungen p, q; um also alle ganzzahligen Lösungen von (44) zu finden, hat man zunächst die ganzzahligen Lösungen von (48) zu ermitteln.

2) Im Falle nun $b^2 - ac < 0$ ist, giebt es, wenn überhaupt, jedenfalls nur eine endliche Anzahl ganzzahliger Lösungen

p, q dieser Gleichung, die nach der Lehre von der Darstellung der Zahlen durch binäre Formen ermittelt werden können, und da ihnen nach den Formeln (47) nicht immer ganzzahlige x, y zu entsprechen brauchen, hat auch die Gleichung (44), wenn überhaupt Lösungen, jedenfalls nur eine endliche Anzahl ganzzahliger Lösungen.

3) Sei endlich $b^2 - ac > 0$. Dann unterscheide man die zwei Fälle, in denen $b^2 - ac$ eine Quadratzahl oder keine Quadratzahl ist.

Ist zunächst $b^2 - ac = \varkappa^2$, so ist die Gleichung (48), wenn $a \gtrless 0$ ist, gleichbedeutend mit der andern:

$$(ap + bq)^2 - \varkappa^2 q^2 = aM$$

oder auch mit dieser:

$$(ap + bq + \varkappa q)(ap + bq - \varkappa q) = aM.$$

Wenn daher M von Null verschieden ist und $r \cdot s$ irgend eine Zerlegung von M in zwei Faktoren, so wird man alle möglichen ganzzahligen Auflösungen von (48) finden, wenn man die sämmtlichen Paare von Gleichungen

$$ap + (b + \varkappa)q = r$$
$$ap + (b - \varkappa)q = s$$

in ganzen Zahlen p, q auflöst, was nur eine endliche Anzahl von ganzzahligen Auflösungen liefern kann.

Ist dagegen $M = 0$, so hat man p, q entweder als ganzzahlige Auflösung der Gleichung

$$ap + (b + \varkappa)q = 0$$

oder der Gleichung

$$ap + (b - \varkappa)q = 0$$

zu bestimmen und findet demnach jedenfalls p, q unter der Form

$$p = Az, \quad q = Bz,$$

in welcher A, B zwei relative Primzahlen bedeuten. Somit erhalten x, y nach den Formeln (47) die Ausdrücke

$$x = \frac{Az + cd - be}{D}, \quad y = \frac{Bz + ae - bd}{D},$$

in denen zur Abkürzung D steht für $b^2 - ac$. Hieraus er-

giebt sich die Gleichung

$$D(\mathfrak{a}x + \mathfrak{b}y) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd),$$

wenn man die ganzen Zahlen $\mathfrak{a}$, $\mathfrak{b}$ der Gleichung

$$\mathfrak{a}A + \mathfrak{b}B = 1$$

gemäss wählt; man erkennt darnach, dass die unbestimmte ganze Zahl z, wenn x, y ganzzahlig werden sollen, die Gestalt

$$z = Du + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$$

haben muss; für solche z aber erhält man

$$x = Au + \mathfrak{b} \cdot \frac{A(bd - ae) - B(be - cd)}{D}$$

$$y = Bu - \mathfrak{a} \cdot \frac{A(bd - ae) - B(be - cd)}{D};$$

ist also der hier auftretende Bruch einer ganzen Zahl gleich, so giebt es unendlich viele, im entgegengesetzten Falle keine ganzzahligen Auflösungen der Gleichung (44).

Wenn $a = 0$ ist, nimmt die Gleichung (48) die Gestalt an:

$$(2bp + q)q = M;$$

ist dann M von Null verschieden, so kann es wieder nur eine endliche Anzahl ganzzahliger Lösungen geben. Für $M = 0$ aber hat man p, q entweder als ganzzahlige Lösungen der Gleichung

$$2bp + q = 0$$

zu wählen und gelangt zu genau entsprechenden Resultaten, wie im Falle $a \gtrless 0$; oder man hat $q = 0$, p beliebig, und dann findet man wieder die gleichen Resultate, bei denen nur $A = 1$, $B = 0$ und entsprechend $\mathfrak{a} = 1$, $\mathfrak{b}$ beliebig zu nehmen ist, also

$$x = u + \mathfrak{b} \cdot \frac{d}{b}, \quad y = -\frac{d}{b},$$

also unendlich viel oder keine Lösungen, je nachdem $\frac{d}{b}$ eine ganze Zahl ist, oder nicht.

Sei nun zuletzt $b^2 - ac$ eine positive, aber keine quadratische Zahl. Bedeutet dann δ den grössten gemeinsamen Theiler von a, b, c, so muss auch M, wenn die Gleichung (48) auflösbar sein soll, diesen Theiler besitzen, und

die Gleichung ist, wenn

$$a = a'\delta, \quad b = b'\delta, \quad c = c'\delta, \quad M = M'\delta$$

gesetzt wird, gleichbedeutend mit dieser anderen:

$$a'p^2 + 2b'pq + c'q^2 = M'; \tag{49}$$

wir setzen

$$D' = b'^2 - a'c'.$$

Bezeichnet nun $\varDelta^2$ jeden quadratischen Theiler von M', so erhält man die **sämmtlichen** Darstellungen von M' aus den **eigentlichen** Darstellungen p', q' der Zahlen $\frac{M'}{\varDelta^2}$ durch die Formeln

$$p = \varDelta p', \quad q = \varDelta q'.$$

Sei $\sigma = 1$ oder 2, je nachdem die Form (a', b', c') eigentlich- oder uneigentlich-primitiv ist; bekanntlich bilden dann die eigentlichen Darstellungen von $\frac{M'}{\varDelta^2}$, wenn es deren überhaupt giebt, eine oder mehrere **Gruppen** von Darstellungen von der Form

$$p' = \frac{\alpha t - (b'\alpha + c'\gamma)u}{\sigma}, \quad q' = \frac{\gamma t + (a'\alpha + b'\gamma)u}{\sigma},$$

wo α, γ **eine** solche Darstellung ist und t, u alle ganzzahligen Auflösungen der Gleichung

$$t^2 - D'u^2 = \sigma^2 \tag{50}$$

bedeuten. Für diese Werthe von p', q' erhält man aus (47) als zugehörige Werthe von x, y Ausdrücke von folgender Form:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + \sigma cd - \sigma be}{\sigma D}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + \sigma ae - \sigma bd}{\sigma D}. \tag{51}$$

Um hiernach sämmtliche ganzzahlige Lösungen x, y der Gleichung (44) zu finden, hat man nur für jeden quadratischen Theiler, für welchen $\frac{M'}{\varDelta^2}$ eine eigentliche Darstellung durch die Form (a', b', c') gestattet und für jede Gruppe solcher Darstellungen die Ausdrücke (51) aufzustellen und nun in dieselben **diejenigen Auflösungen der Gleichung** (50) **einzusetzen, welche sie ganzzahlig machen.**

Um dies letztere zu erreichen, bemerke man, dass, wenn T, U die Fundamentallösung der Gleichung (50) ist, sämmt-

liche Auflösungen t, u durch die Formel

$$\frac{t+u\sqrt{D'}}{\sigma} = \pm\left(\frac{T+U\sqrt{D'}}{\sigma}\right)^n$$

$$\text{für } n = 0, \pm 1, \pm 2, \cdots$$

gegeben werden. Setzen wir

$$\frac{t_n+u_n\sqrt{D'}}{\sigma} = \left(\frac{T+U\sqrt{D'}}{\sigma}\right)^n$$

und bezeichnen mit m irgend welche ganze Zahl. Da es unendlich viel Systeme t_n, u_n giebt, muss es auch unendlich viel derselben geben, welche dieselbe Restcombination (mod. m) aufweisen; sei z. B.

$$t_{n+h} \equiv t_n, \quad u_{n+h} \equiv u_n \pmod{m};$$

aus den Formeln

$$t_{n\pm 1} = \frac{t_n T \pm u_n U D'}{\sigma}, \quad u_{n\pm 1} = \frac{\pm t_n U + u_n T}{\sigma}$$

sowie den entsprechenden

$$t_{n+h\pm 1} = \frac{t_{n+h} T \pm u_{n+h} U D'}{\sigma}, \quad u_{n+h\pm 1} = \frac{\pm t_{n+h} U + u_{n+h} T}{\sigma}$$

erkennt man dann die Richtigkeit der Congruenzen

$$\sigma t_{n\pm 1} \equiv \sigma t_{n+h\pm 1}, \quad \sigma u_{n\pm 1} \equiv \sigma u_{n+h\pm 1} \pmod{m},$$

und folglich ergeben sich, wenn $\sigma = 1$ oder auch wenn $\sigma = 2$ und zugleich m gerade ist, die Congruenzen

$$\left.\begin{aligned} t_{n+h} &\equiv t_n, & u_{n+h} &\equiv u_n \\ t_{n+h\pm 1} &\equiv t_{n\pm 1}, & u_{n+h\pm 1} &\equiv u_{n\pm 1} \end{aligned}\right\} \left(\text{mod. } \frac{m}{\sigma}\right).$$

Wir wählen nun für m den Werth $\sigma^2 \cdot D$. Vermittelst des erhaltenen Resultates folgt dann nach den leicht erweisbaren Beziehungen

$$t_n = 2\frac{T}{\sigma} t_{n-1} - t_{n-2}, \quad u_n = 2\frac{T}{\sigma} u_{n-1} - u_{n-2}$$

allgemein

$$t_n \equiv t_r, \quad u_n \equiv u_r \pmod{\sigma D},$$

wenn r den kleinsten positiven Rest von n (mod. h) bezeichnet. Um daher aus den Formeln (51) diejenigen auszuscheiden, denen ganzzahlige x, y zugehören, genügt es, für t, u die Systeme $t = \pm t_r$, $u = \pm u_r$ zu versuchen; wählt man die-

jenigen der letzteren aus — sie mögen t_ϱ, u_ϱ genannt werden — welche x, y ganzzahlig machen, so hat man in (51) diejenigen Lösungen der Pell'schen Gleichung zu setzen, für welche

$$t \equiv t_\varrho, \quad u \equiv u_\varrho \pmod{\sigma D}$$

ist, und nur diese.

Hiermit ist aber die vollständige Auflösung der Gleichung (44) geleistet.

9. Schliesslich mögen hier noch die Bedingungen angegeben werden, welche nothwendig und hinreichend dafür sind, dass die allgemeine quadratische Gleichung (2):

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx' = 0,$$

wenn in ihr f eine unbestimmte Form bedeutet, ganzzahlige Auflösungen besitze. Diese können aus den für die einfachere Gleichung

$$ax^2 + a'x'^2 + a''x''^2 = 0$$

nach Legendre mitgetheilten Bedingungen ohne Mühe hergeleitet werden und sind zuerst von St. Smith folgendermassen ausgesprochen worden*), wobei die vorkommenden Zeichen die frühere Bedeutung haben, für jede Zahl n aber unter dem Zeichen $\overline{n}$ der Quotient aus derselben und dem grössten in ihr aufgehenden Quadrate verstanden wird:

Sei ω jeder Primfaktor von $\overline{\Omega}$, der nicht in $\overline{\Delta}$, δ jeder Primfaktor von $\overline{\Delta}$, der nicht in $\overline{\Omega}$, und r jeder Primfaktor, der sowohl in $\overline{\Omega}$ als in $\overline{\Delta}$ und folglich nicht in $\overline{\Omega\Delta}$ aufgeht; dann ist die Gleichung (2) auflösbar oder nicht, jenachdem die auf alle jene Primfaktoren bezogenen Gleichungen

$$\left(\frac{-\overline{\Delta} f}{\omega}\right) = 1, \quad \left(\frac{-\overline{\Omega}\mathfrak{F}}{\delta}\right) = 1, \quad \left(\frac{-\overline{\Omega\Delta} \cdot f\mathfrak{F}}{r}\right) = 1$$

erfüllt sind oder nicht.

Indem wir immer an der Voraussetzung ungerader Inva-

---

*) St. Smith, on the Criterion of Resolubility in Integral Numbers of the Indeterminate Equation

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx' = 0,$$

in den Proceedings of the R. Society of London, vol. 13, S. 110.

rianten $\mathfrak{Q}, \Delta$ festhalten, wollen wir die Richtigkeit dieser Aussage beweisen*).

Da durch äquivalente Formen die gleichen Zahlen dargestellt werden, darf die Form f in der Gleichung (2) durch irgend eine äquivalente ersetzt werden. Andererseits ist in nr. 11 des dritten Capitels gezeigt worden, dass f einer Form äquivalent ist, in der der erste Coefficient, sowie der dritte Coefficient in ihrer Reciproken positiv, prim gegen $2\mathfrak{Q}\Delta$ und auch prim gegen einander sind. Zur Vereinfachung darf man daher annehmen, dass in der Gleichung (2) der Coefficient a sowie die durch die Gleichung

$$aa' - b''^2 = \mathfrak{Q} \cdot \mathfrak{A}''$$

definirte Zahl $\mathfrak{A}''$ positiv, prim gegen $2\mathfrak{Q}\Delta$ und prim unter einander sind. Nach nr. 1 ist ferner die Gleichung (2) gleichbedeutend mit der folgenden:

$$\mathfrak{A}''(ax + b''x' + b'x'')^2 + \mathfrak{Q}(\mathfrak{A}''x' - \mathfrak{B}x'')^2 + a\mathfrak{Q}\Delta x''^2 = 0.$$

Diese nun hat die Gestalt der Gleichung (1):

$$\mathfrak{A}''u^2 + \mathfrak{Q}v^2 + a\mathfrak{Q}\Delta w^2 = 0$$

und lässt sich auf eine andere reduciren, welche die Voraussetzungen des Legendre'schen Criteriums erfüllt. Zunächst kann sie durch die folgende:

$$\overline{\mathfrak{A}''}u^2 + \overline{\mathfrak{Q}}v^2 + \overline{a\mathfrak{Q}\Delta}w^2 = 0$$

ersetzt werden. Wenn man aber mit R den grössten positiven gemeinsamen Theiler von $\overline{\mathfrak{Q}}$ und $\overline{\Delta}$ bezeichnet, sodass man

$$\overline{\mathfrak{Q}} = R \cdot \mathfrak{Q}_1, \quad \overline{\Delta} = R \cdot \Delta_1$$

setzen kann, so findet sich offenbar

$$\overline{\mathfrak{Q}\Delta} = \mathfrak{Q}_1\Delta_1.$$

Die vorige Gleichung erfordert also, dass u theilbar sei durch $\mathfrak{Q}_1$; sie ist mithin zugleich auflösbar resp. nicht auflösbar mit dieser anderen:

$$\overline{\mathfrak{A}''}\mathfrak{Q}_1 \cdot U^2 + R \cdot V^2 + \bar{a}\Delta_1 \cdot W^2 = 0,$$

---

*) Dies ist bereits von A. Meyer gethan worden in seiner Abh. über die Classenanzahl derjenigen ternären quadratischen Formen, durch welche die Null rational darstellbar ist, Journ. f. Math. 98 S. 177.

in welcher nun die Coefficienten nach den gemachten Voraussetzungen zu je zweien prim und ohne quadratischen Theiler sind. Zur Auflösung der letzten und somit auch der gegebenen Gleichung in ganzen oder allgemeiner rationalen Zahlen ist folglich nothwendig und hinreichend, dass

$$\begin{array}{lll} -\bar{a}R\Delta_1 & = -\overline{a\Delta} & \text{qu. Rest von } \bar{\mathfrak{A}}''\mathfrak{Q}_1 \\ -a\bar{\mathfrak{A}}''\mathfrak{Q}_1\Delta_1 & = -a\bar{\mathfrak{A}}''\cdot\overline{\mathfrak{Q}\Delta} & \quad " \quad " \quad " \quad R \\ -\bar{\mathfrak{A}}''\cdot R\mathfrak{Q}_1 & = -\bar{\mathfrak{A}}''\cdot\bar{\mathfrak{Q}} & \quad " \quad " \quad " \quad \bar{a}\Delta_1 \end{array}$$

ist. Da zufolge der Beziehung

$$\mathfrak{A}'\mathfrak{A}'' - \mathfrak{B}^2 = \Delta a$$

immer $-\overline{a\Delta}$ qu. Rest von $\bar{\mathfrak{A}}''$ ist, sowie wegen der Beziehung

$$\mathfrak{Q}\mathfrak{A}'' = aa' - b''^2$$

stets $-\bar{\mathfrak{A}}''\cdot\bar{\mathfrak{Q}}$ qu. Rest von a, können die vorstehenden Bedingungen einfacher auch so gefasst werden:

$$\begin{array}{ll} -\overline{a\Delta} & \text{qu. Rest von } \mathfrak{Q}_1 \\ -a\bar{\mathfrak{A}}''\cdot\overline{\mathfrak{Q}\Delta} & \quad " \quad " \quad " \quad R \\ -\bar{\mathfrak{A}}''\cdot\bar{\mathfrak{Q}} & \quad " \quad " \quad " \quad \Delta_1. \end{array}$$

Beachtet man also, dass a ein Werth der Form f, $\mathfrak{A}''$ ein solcher von $\mathfrak{F}$ und von $\bar{\mathfrak{A}}''$ nur um einen quadratischen, zu $2\mathfrak{Q}\Delta$ primen Faktor verschieden ist, so sind diese Bedingungen in der That mit den nach St. Smith angegebenen durchaus identisch.

Neuntes Capitel.

Unbestimmte Formen. Classenzahl eines Geschlechts.

1. Während bei den bestimmten Formen das Maass eines Geschlechts, scheint bei den unbestimmten die Anzahl seiner Classen der einfachere Begriff zu sein. Eisenstein hat zuerst die Vermuthung ausgesprochen, dass jedes Geschlecht unbestimmter Formen nur aus einer einzigen Classe von Formen

bestehe*), und die Arbeiten von A. Meyer haben diese Vermuthung in gewissem Umfange bestätigt. Das gegenwärtige Capitel soll von den bezüglichen Untersuchungen des jüngst leider so frühe der Wissenschaft entrissenen**) Forschers dasjenige mittheilen, was einfach darstellbar ist.

A. Meyers erste Arbeit über den bezeichneten Gegenstand gründet sich auf einen die Pell'sche Gleichung betreffenden Satz, dem er in einer späteren Arbeit allgemeinere Fassung gegeben hat, als wir hier bedürfen***). In seiner engeren Fassung lautet er, wie folgt: Ist Δ eine positive ungerade Zahl, so giebt es unendlich viel ungerade Primzahlen p, q so beschaffen, dass für die Fundamentalauflösung T, U der Pell'schen Gleichung

$$(1) \qquad t^2 - pq\Delta u^2 = 1$$

$T \pm 1$ nicht durch pq theilbar ist.

1) Die Primzahlen p, q dürfen als solche vorausgesetzt werden, die nicht in Δ aufgehen; setzt man also zur Abkürzung $pq = a$, so ist a prim zu 2Δ. Man verstehe ferner unter S^2 das grösste in Δ aufgehende Quadrat, sodass, wenn

$$\Delta = D \cdot S^2$$

geschrieben wird, D aus lauter verschiedenen ungeraden Primfaktoren besteht. Aus der Gleichung

$$(T+1)(T-1) = aDS^2U^2$$

folgt dann unter der Annahme, dass $T+1$ oder $T-1$ durch a aufgeht, eines der beiden Systeme von Gleichungen:

entweder

$$T \pm 1 = \delta \cdot 2\tau^2, \quad T \mp 1 = ad \cdot 2v^2,$$

---

*) Eisenstein, Tabelle der reducirten positiven ternären quadratischen Formen u. s. w. im Journ. f. Math. 41 S. 168.

**) Kurz bevor der Verfasser dieses Capitel ausarbeitete, ging ihm die ihn tief betrübende Mittheilung zu, dass Arnold Meyer am 7. Juli d. J. verstorben sei.

***) A. Meyer, zur Theorie der unbestimmten ternären quadratischen Formen, Inauguraldissertation, Zürich 1871. Die spätere Arbeit, über eine Eigenschaft der Pell'schen Gleichung, findet sich in der Vierteljahrsschrift der Züricher naturforsch. Gesellsch. v. J. 1888. Siehe auch seine Abhandlung im 108. Bd. des Journ. f. Math.

wo

$$d\delta = D, \quad 2\tau v = SU$$

ist, also

(2) $$\delta\tau^2 - adv^2 = \pm 1$$

oder

$$T \pm 1 = \delta \cdot \tau^2, \quad T \mp 1 = ad \cdot v^2,$$

wo

$$d\delta = D, \quad \tau v = SU$$

ist, also

(2a) $$\delta\tau^2 - adv^2 = \pm 2.$$

Lässt sich demnach $a = pq$ so wählen, dass keine der Gleichungen (2) oder (2a) statthaben kann, so wird für solche Werthe der Primzahlen p, q der behauptete Satz zutreffend sein.

Setzt man nun, um dies näher zu untersuchen,

(3) $$f(\delta) = \delta x^2 - ady^2$$

und für δ sämmtliche positive Theiler von D, so erhält man, unter n die Anzahl der Primfaktoren von D verstanden, 2^n quadratische Formen

(4) $$f(1), f(\delta), f(\delta'), \ldots$$

mit der gemeinsamen Determinante aD, welche sich zu je zweien wieder zu einer Form derselben Reihe zusammensetzen, da, wenn

$$f(\delta') = \delta' x'^2 - ad' y'^2$$

gesetzt wird, wo $\delta' d' = D$, leicht die Gleichung

$$f(\delta)\, f(\delta') = \frac{\delta\delta'}{\varepsilon^2}\left(\varepsilon x x' + \frac{\varepsilon a D}{\delta\delta'} y y'\right)^2 - \frac{aD\varepsilon^2}{\delta\delta'}\left(\frac{\delta'}{\varepsilon} x' y + \frac{\delta}{\varepsilon} x y'\right)^2,$$

in welcher ε den grössten gemeinsamen Theiler von δ, δ' bedeutet, d. i. die Gleichung

(5) $$f(\delta) \cdot f(\delta') = f\left(\frac{\delta\delta'}{\varepsilon^2}\right)$$

bestätigt wird.

Jeder der Formen (4) kommen in Bezug auf die n verschiedenen Primfaktoren von D ebenso viel quadratische Geschlechtscharaktere zu, deren Gesammtheit wir ihr Geschlecht in Bezug auf D nennen wollen, und die insbesondere für die Form $f(1)$ sämmtlich der positiven Einheit gleich sind. Es

kann aber zunächst gezeigt werden, dass bei geeigneter Wahl von a *jedem* der 2^n möglichen Geschlechter in Bezug auf D je *eine* der 2^n Formen (4) zugehört. Dies ist selbstverständlich für $D = 1$, wo es nur die eine Form $f(1)$ giebt. Wir nehmen es als bereits bewiesen an für eine Zahl

$$D' = p_1 p_2 \cdots p_{n-1},$$

die aus $n - 1$ Primfaktoren besteht, und zeigen, dass es dann auch gilt für die Zahl

$$D = p_1 p_2 \cdots p_{n-1} p_n.$$

Der Zahl D' entsprechen 2^{n-1} Formen

$$f'(\delta') = \delta' x^2 - a' d' y^2,$$

wo $d'\delta' = D'$ und die Zahl a' so gewählt gedacht ist, dass alle diese Formen zu verschiedenen Geschlechtern in Bezug auf D' gehören d. h. dass die Symbole

$$\left(\frac{f'}{p_1}\right), \left(\frac{f'}{p_2}\right), \cdots \left(\frac{f'}{p_{n-1}}\right)$$

für keine zwei von ihnen dieselbe Combination von Einheiten darbieten. Jenen Formen entsprechen aber **erstens** diejenigen 2^{n-1} Formen (4), welche die Gestalt haben:

$$f(\delta') = \delta' x^2 - a d' p_n y^2.$$

Genügt nun a den Bedingungen:

$$\left(\frac{a p_n}{p_1}\right) = \left(\frac{a'}{p_1}\right), \left(\frac{a p_n}{p_2}\right) = \left(\frac{a'}{p_2}\right) \cdots \left(\frac{a p_n}{p_{n-1}}\right) = \left(\frac{a'}{p_{n-1}}\right), \tag{6}$$

so leuchtet ein, dass

$$\left(\frac{f}{p_1}\right) = \left(\frac{f'}{p_1}\right), \left(\frac{f}{p_2}\right) = \left(\frac{f'}{p_2}\right) \cdots \left(\frac{f}{p_{n-1}}\right) = \left(\frac{f'}{p_{n-1}}\right) \tag{7}$$

sein wird, daher gehören dann diese 2^{n-1} der Formen (4) in Bezug auf D' ebenso viel verschiedenen Geschlechtern an und nur für **eine** von ihnen können die sämmtlichen Symbole (7) gleich $+1$ sein. Dies ist die Form $f(1)$, für welche auch noch der auf p_n bezügliche Charakter den gleichen Werth hat.

Zweitens entsprechen den 2^{n-1} Formen $f'(\delta')$ ebenso viel Formen (4) von der Gestalt

$$f(\delta' p_n) = \delta' p_n x^2 - a d' y^2.$$

Aus dieser Gleichung findet sich, sobald p_x einer der Primfaktoren $p_1, p_2, \dots p_{n-1}$ ist, mit Beachtung der Bedingungen (6) die folgende:

$$\left(\frac{f}{p_x}\right) = \left(\frac{f'}{p_x}\right) \cdot \left(\frac{p_n}{p_x}\right),$$

sodass auch diese 2^{n-1} der Formen (4) zu verschiedenen Geschlechtern in Bezug auf D' gehören und wieder nur für eine derselben sämmtliche Symbole $\left(\frac{f}{p_x}\right)$ gleich $+1$ sein könnten. Ferner aber ist

$$\left(\frac{f}{p_n}\right) = \left(\frac{-ad'}{p_n}\right);$$

wird demnach der quadratische Charakter von a bezüglich der Primzahl p_n so gewählt, dass für die erwähnte einzige Form, falls sie vorhanden,

(6a) $$\left(\frac{-ad'}{p_n}\right) = -1$$

ist, so giebt es unter den sämmtlichen 2^n Formen (4) nur eine einzige — die Form $f(1)$ — deren sämmtliche Charaktere in Bezug auf D gleich $+1$ sind. Wegen (5) gehören dann alle diese Formen verschiedenen Geschlechtern in Bezug auf D an; denn gehörten zwei, für welche δ, δ' von einander also $\frac{\delta\delta'}{\varepsilon^2}$ von 1 verschieden ist, demselben Geschlechte an, so wäre die Form $f\left(\frac{\delta\delta'}{\varepsilon^2}\right)$ noch eine zweite Form, für welche sämmtliche Charaktere in Bezug auf D gleich $+1$ wären. — Hiermit ist der behauptete Satz allgemein bewiesen.

2) Nunmehr kann aber a weiter so bestimmt werden, dass keine der Formen (4) eine der Zahlen -1, ± 2 darzustellen vermag. Die Zahl $+1$, die für jede der Primzahlen $p_1, p_2, \dots p_n$ den quadratischen Charakter $+1$ hat, kann offenbar nur durch

$$f(1) = x^2 - aDy^2$$

dargestellt werden. Fände aber die der Annahme $\delta = 1$ entsprechende Gleichung (2):

(8) $$\tau^2 - aDv^2 = 1$$

statt, so könnte v nicht durch S theilbar sein, denn, wäre $v = Su$, so hätte man die Gleichungen

$$\tau^2 - a\Delta u^2 = 1$$

$$T = \tau^2 + a\Delta u^2, \quad U = 2\tau u$$

und T, U wäre nicht die Fundamentalauflösung der Gleichung (1). Der Gleichung $2\tau v = SU$ zufolge müsste daher wenigstens ein Primfaktor s von S und zwar, der Gleichung (8) wegen, einer derjenigen Primfaktoren $s_1, s_2, \ldots s_r$, welche nicht zugleich in D enthalten sind, nicht in v aber in τ aufgehen, und man hätte nach jener Gleichung

$$\left(\frac{-aD}{s}\right) = 1.$$

Wählt man mithin a so, dass die Bedingungen

$$(9) \qquad \left(\frac{-aD}{s_1}\right) = -1, \ \left(\frac{-aD}{s_2}\right) = -1, \cdots \left(\frac{-aD}{s_r}\right) = -1$$

erfüllt werden, so ist damit die Gleichung (8) unmöglich gemacht.

Man bemerke nun, bevor wir weiter gehen, dass, wenn schon durch die Bedingungen (6), (6a) und (9) über den quadratischen Charakter des Produkts $a = pq$ bezüglich der in Δ aufgehenden Primfaktoren verfügt worden ist, dabei gleichwohl die bezüglichen Charaktere eines der Primfaktoren p, q noch ganz willkürlich bleiben. Auch dürfen wir noch ihre Charaktere bezüglich des Modulus 8 ganz nach Belieben annehmen. Es ist zu zeigen, dass durch geeignete Wahl der genannten Charaktere auch die übrigen der Gleichungen (2) und (2a) unmöglich gemacht werden können.

Wählt man zuerst

$$p \equiv 5, \ q \equiv 3, 7 \quad \text{oder} \ p \equiv 3, \ q \equiv 7 \pmod{8},$$

so wird offenbar schon jede der Gleichungen

$$(10) \qquad \tau^2 - aDv^2 = -1, +2, -2$$

unmöglich, da jede derselben als Congruenz (mod. p oder q) aufgefasst nach wenigstens einem dieser Moduln einen Widerspruch ergäbe.

3) Dem unter 1) Bewiesenen zufolge giebt es aber unter den Formen (4) drei solche: $f(\delta)$, $f(\delta')$, $f(\delta'')$, deren Charaktere in Bezug auf die Primfaktoren von D mit denjenigen der Zahlen -1, $+2$, -2 resp. übereinstimmen; diese Formen

sind durch die Gleichung

$$f(\delta)\,f(\delta') = f\left(\frac{\delta\delta'}{\varepsilon^2}\right) = f(\delta'')$$

mit einander verbunden und brauchen nicht alle drei verschieden von einander zu sein. Sie sind zudem die einzigen Formen (4), durch welche möglicherweise die Zahl -1, $+2$, -2 resp. dargestellt werden kann. Durch die unter 1) getroffene Bestimmung für die Zahlen p, q sind offenbar die Werthe der Symbole $\left(\frac{\delta}{pq}\right)$, $\left(\frac{\delta'}{pq}\right)$ also auch

$$\left(\frac{\delta''}{pq}\right) = \left(\frac{\delta}{pq}\right) \cdot \left(\frac{\delta'}{pq}\right)$$

zugleich bestimmt. Man wähle nun,

wenn $\left(\frac{\delta}{pq}\right) = 1$, $\left(\frac{\delta'}{pq}\right) = 1$ ist, $\left(\frac{\delta}{p}\right) = 1$, $\left(\frac{\delta'}{p}\right) = 1$ und
entweder $p \equiv 5$, $q \equiv 3$ oder $p \equiv 3$, $q \equiv 7 \pmod{8}$;

wenn $\left(\frac{\delta}{pq}\right) = -1$, $\left(\frac{\delta'}{pq}\right) = -1$ ist,
$\left(\frac{\delta}{p}\right) = -1$, $\left(\frac{\delta'}{p}\right) = 1$ und
entweder $p \equiv 5$, $q \equiv 3$ oder $p \equiv 3$, $q \equiv 7 \pmod{8}$;

wenn $\left(\frac{\delta}{pq}\right) = -1$, $\left(\frac{\delta'}{pq}\right) = +1$ ist,
$\left(\frac{\delta}{p}\right) = -1$, $\left(\frac{\delta'}{p}\right) = 1$ und
entweder $p \equiv 5$, $q \equiv 7$ oder $p \equiv 3$, $q \equiv 7 \pmod{8}$;

wenn $\left(\frac{\delta}{pq}\right) = 1$, $\left(\frac{\delta'}{pq}\right) = -1$ ist, $\left(\frac{\delta}{p}\right) = 1$, $\left(\frac{\delta'}{p}\right) = 1$ und
$p \equiv 5$, $q \equiv 3 \pmod{8}$.

Dann ist ohne Mühe zu bestätigen, dass durch solche, mit der früheren verträgliche Bestimmung für die Zahlen p, q die Gleichungen

$$(11) \qquad f(\delta) = -1, \quad f(\delta') = 2, \quad f(\delta'') = -2$$

und damit zugleich die noch übrigen Gleichungen (2) und (2a) unmöglich gemacht werden.

Man sieht zudem, was für die Folge hervorzuheben ist, dass, während stets $q \equiv 3 \pmod{4}$ ist, nach

Belieben $pq \equiv 1$ oder $\equiv 3 \pmod{4}$ gewählt werden kann. Im vierten der unterschiedenen Fälle freilich ist

$$pq \equiv 3 \pmod{4}.$$

Ersetzt man aber die Restbestimmung der Zahlen $p, q \pmod{8}$, durch welche unter 2) die Gleichungen (10) unmöglich gemacht wurden, in diesem Falle durch die folgende:

wenn D einen Primfaktor $8n + 3$ enthält,

$$p \equiv q \equiv 7 \pmod{8},$$

wenn D einen Primfaktor $8n + 7$ enthält,

$$p \equiv q \equiv 3 \pmod{8},$$

wenn D einen Primfaktor $8n + 5$ enthält,

$$p \equiv q \equiv 3, 7 \pmod{8},$$

so erkennt man leicht, dass dann nicht nur jedesmal die Gleichungen (10), sondern auch mit den Gleichungen (11) die noch übrigen der Gleichungen (2) und (2a) wieder unmöglich gemacht werden; gleichzeitig aber wird jetzt

$$pq \equiv 1 \pmod{4}.$$

Falls endlich D nur Primfaktoren $8n + 1$ enthält, bedarf es überhaupt ausser den unter 1) und 2) getroffenen Bestimmungen für p, q keiner weiteren mehr; denn in diesem Falle leuchtet ein, dass keine der noch übrigen Gleichungen (2) und (2a) möglich ist, weil sonst für ein $\delta > 1$ sämmtliche quadratische Charaktere von $f(\delta)$ bezüglich der Primfaktoren p_1, $p_2, \ldots p_n$ gleich $+1$ wären, gegen die unter 1) getroffene Bestimmung.

Durch dies Alles sind für die Primzahlen p, q gewisse Reste mit Bezug auf 8 sowie auf die verschiedenen in Δ aufgehenden Primfaktoren festgestellt, welche die Gewissheit geben, dass die Gleichungen (2) und (2a) unmöglich sind*). Dadurch sind die geeigneten Primzahlen p, q auf zwei bestimmte arithmetische Reihen verwiesen; letztere aber enthalten nach dem Satze von der arithmetischen Progression auch in der That unendlich viel positive Primzahlen p resp. q, und jedem

*) Uebrigens ist diese Bestimmung der Reste nicht die einzig zulässige, wie aus A. Meyer's zweiter Arbeit näher zu ersehen ist.

solchen Paare p, q von Primzahlen kommt die im Satze von A. Meyer behauptete Beschaffenheit zu.

2. Ein zweiter Hilfssatz, dessen wir bedürfen, besagt Folgendes: Wenn zwei eigentlich-primitive binäre quadratische Formen φ, φ_1 von einer von ± 1 verschiedenen Determinante, die, wenn letztere negativ ist, als positive Formen vorausgesetzt werden, desselben Geschlechts sind, so giebt es unendlich viel Primzahlen p', q' der Art, dass ihr Produkt $p'q'$ durch beide Formen darstellbar ist.

Sind nämlich C, C_1 die Classen des Geschlechts, denen φ, φ_1 angehören, so gehört die Classe $C \cdot C_1$ ins Hauptgeschlecht, entsteht also durch Duplikation einer eigentlich-primitiven Classe L der gleichen Determinante, sodass man setzen kann

$$C \cdot C_1 = L^2.$$

Wird dann noch die ebenfalls eigentlich-primitive Classe L_1 so gewählt, dass $L \cdot L_1 = C$ ist, so findet sich $L \cdot L_1^{-1} = C_1$. Nun stellen die entgegengesetzten Classen L_1, L_1^{-1} genau dieselben Zahlen dar, und durch die Classen L, L_1 können, einem Dirichlet'schen Satze zufolge, unendlich viel Primzahlen p', q' resp. eigentlich dargestellt werden, deren quadratische Charaktere mit den Geschlechtscharakteren der Classen resp. übereinstimmen. Den vorigen Gleichungen zufolge ist demnach das Produkt $p'q'$ jedes solchen Paares von Primzahlen sowohl durch φ als durch φ_1 eigentlich darstellbar.

Wenn hierbei für die Determinante der Formen kein quadratischer Charakter (mod. 4) in Frage kommt, dürfen offenbar die beiden Primzahlen nach Belieben von der Form $4n + 1$ oder $4n + 3$ vorausgesetzt werden.

Tritt aber ein solcher Charakter auf und ist er für das Geschlecht der Formen φ, φ_1 der Charakter 3 (mod. 4), so muss

$$p'q' \equiv 3 \pmod{4}$$

sein, demnach wird immer noch eine der beiden Primzahlen von der Form $4n + 3$, die andere von der Form $4n + 1$ sein.

Ist dagegen der Charakter der Formen φ, φ_1 der Charakter 1 (mod. 4), so muss

$$p'q' \equiv 1 \pmod{4}$$

sein und man hat nothwendig

$$\text{entweder } p' \equiv q' \equiv 1 \quad \text{oder } p' \equiv q' \equiv 3 \pmod{4}.$$

Alsdann sind zwei Fälle zu unterscheiden. Wenn erstens eine ambige Classe A vom Charakter 3 (mod. 4) vorhanden ist, so darf man nach Belieben das eine oder das andere annehmen. Denn, da sowohl $C \cdot C_1 = L^2$ als auch $C \cdot C_1 = (LA)^2$ ist, darf man im obigen Räsonnement L durch LA ersetzen, und die Charaktere dieser beiden Classen (mod. 4) sind entgegengesetzt. — Wenn aber zweitens jede ambige Classe den Charakter 1 (mod. 4) hat, so zerfallen die Classen des Geschlechts der Formen φ, φ_1 in zwei Categorieen: für zwei Classen derselben Categorie bestehen die dargestellten Produkte $p'q'$ aus Primzahlen $4n+1$, für zwei Classen verschiedener Categorie aus Primzahlen $4n+3$. Um dies zu beweisen, seien C, C_1, C_2 irgend drei Classen des Geschlechts und

$$C \cdot C_1 = L^2, \cdot C \cdot C_2 = M^2 \quad \text{also } C_1 \cdot C_2 = (LMC^{-1})^2.$$

Sind für beide Classenpaare C, C_1 und C, C_2 die Zahlen p', q' congruent 1, oder für beide congruent 3 (mod. 4), so stimmen die Charaktere von L, M (mod. 4) überein, und da nach der Voraussetzung C den Charakter 1 (mod. 4) hat, gilt Letzteres auch von LMC^{-1}, und folglich sind für das Classenpaar C_1, C_2 die Zahlen p', q' congruent 1. Sind dagegen für eins der Classenpaare C, C_1 und C, C_2 die Zahlen p', q' congruent 1, für das andere congruent 3 (mod. 4), so haben L und M verschiedenen Charakter und LMC^{-1} den Charakter 3 (mod. 4), demnach sind für das Classenpaar C_1, C_2 die Zahlen p', q' congruent 3 (mod. 4). Theilt man folglich die Classen des vorgedachten Geschlechts in zwei Categorieen, jenachdem sie mit C gemeinsam Produkte aus Primzahlen $4n+1$ oder Produkte aus Primzahlen $4n+3$ darstellen, so werden die beiden Categorieen die oben behauptete Eigenschaft haben. Zudem aber enthält auch jede von ihnen wirklich mindestens eine Classe. In der That: in diesem Falle giebt es eine Classe L vom Charakter 1 (mod. 4) und eine solche M vom Charakter 3 (mod. 4), die Classen L^2, M^2 des Hauptgeschlechts aber sind von ein-

ander verschieden, denn sonst wäre $M = L \cdot A$, wo A eine Ambige, was nach der gemachten Voraussetzung über die Ambigen mit dem Charakter von M (mod. 4) unverträglich ist. Da nun die Classen des gedachten Geschlechts, mit C zusammengesetzt, sämmtliche Classen des Hauptgeschlechts hervorbringen, muss es eine möglicherweise mit C identische Classe C_1 und eine von C verschiedene Classe C_2 in jenem geben, so beschaffen, dass $C \cdot C_1 = L^2$, $C \cdot C_2 = M^2$ ist, d. h. eine Classe C_1 der ersten und eine Classe C_2 der zweiten Categorie, w. z. b. w.

Nun sei die Determinante der Formen φ, φ_1 gleich $-\Omega M''$, Δ dieselbe Zahl wie in voriger nr., und die Zahlen $\Omega M''$, Δ relativ prim. Die zwei arithmetischen Reihen, in denen die Primzahlen p, q enthalten waren, werden allein durch die Reste bestimmt, die diesen Zahlen in Bezug auf 8 sowie in Bezug auf die verschiedenen in Δ aufgehenden Primzahlen vorgeschrieben worden sind. Die Reste der Primzahlen p', q' dagegen sind in dem Falle, wo das Geschlecht der Formen φ, φ_1 keinen Charakter (mod. 4) aufweist, nur in Bezug auf die in $\Omega M''$ aufgehenden Primzahlen beschränkt, insofern sie die Geschlechtscharaktere der Classen L, L_1 haben müssen, durch welche sie dargestellt werden. Da die letzteren Primzahlen aber verschieden sind von den ersteren, wird es möglich sein, in den arithmetischen Progressionen für p, q solche Primzahlen zu finden, welche diese für p', q' erforderten Bedingungen erfüllen und damit den beiden Sätzen in dieser und der vorigen nr. gleichzeitig genügen. Tritt aber im Geschlechte der Formen φ, φ_1 ein Charakter (mod. 4) auf und ist er zunächst der Charakter 3 (mod. 4), so ist eine der Zahlen p', q' von der Form $4n + 1$, die andere von der Form $4n + 3$. Im Falle des Charakters 1 (mod. 4) und wenn eine Ambige vom Charakter 3 (mod. 4) vorhanden ist, dürfen beide Primzahlen p', q' von der Form $4n + 3$ vorausgesetzt werden. Es war aber, während q stets $\equiv 3$ (mod. 4) gewählt wurde, zulässig, den Rest von pq (mod. 4) beliebig zu wählen. Daher wird in diesen Fällen es möglich sein, in den beiden bezeichneten Progressionen ein Paar von Primzahlen p, q zu finden, so beschaffen, dass entweder p, q oder q, p allen für

p', q' erforderten Bedingungen und damit den Sätzen in dieser und der vorigen nr. genügen.

Ist dagegen der Charakter des Geschlechts der Formen φ, φ_1 mit Bezug auf 4 der Charakter 1 (mod. 4) und jede Ambige von demselben Charakter, so kann zwar

$$pq \equiv 1 \pmod{4}$$

vorausgesetzt werden, jedoch war dann

$$p \equiv q \equiv 3 \pmod{4},$$

und somit wird nur dann den beiden gedachten Sätzen zugleich genügt werden, wenn auch

$$p' \equiv q' \equiv 3 \pmod{4}$$

d. h. wenn von den beiden Formen φ, φ_1 die eine einer Classe der ersten, die andere einer Classe der zweiten der Categorieen angehört, in welche in diesem Falle die Classen jenes Geschlechtes zerfallen.

3. Diesen auf binäre Formen bezüglichen Hilfssätzen ist ein dritter hinzuzufügen, der sich auf ternäre Formen bezieht und unschwer aus der im dritten Capitel entwickelten Darstellungstheorie erhalten werden kann.

Ist

$$\varphi = (m, n'', m')$$

eine primitive binäre Form mit der Determinante $-\Omega M''$ wo M'' prim gegen $2\Omega\Delta$ gedacht werde, so gehört nach nr. 3 jenes Capitels jede eigentliche Darstellung von φ durch eine ternäre Form der Ordnung (Ω, Δ) zu einer bestimmten Wurzel N, N' der Congruenzen

$$(12) \quad N^2 + \Delta m \equiv 0, \; NN' - \Delta n'' \equiv 0, \; N'^2 + \Delta m' \equiv 0 \pmod{M''}$$

und jede Form jener Ordnung, durch welche φ in solcher Weise darstellbar ist, ist einer Form f äquivalent, deren Reciproke die Gestalt

$$\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$$

hat, wenn M, M', N'' durch die Gleichungen

$$(13) \quad N^2 + \Delta m = MM'', \quad NN' - \Delta n'' = N''M'',$$
$$N'^2 + \Delta m' = M'M''$$

bestimmt werden. Die Zahlen $-N$, $-N'$ bilden aber eine zweite Wurzel derselben Congruenzen (12). Wird φ zu dieser entgegengesetzten Congruenzwurzel gehörig durch eine ternäre Form der Ordnung (Ω, Δ) eigentlich dargestellt, so ist die letztere Form, da die Gleichungen (13) durch eine Vertauschung von N, N' mit $-N$, $-N'$ ungeändert bleiben, einer anderen Form f_1 äquivalent, deren Reciproke

$$\begin{pmatrix} M, & M', & M'' \\ -N, & -N', & N'' \end{pmatrix}$$

ist und in die Reciproke von f übergeht durch die Substitution

$$x = -y, \quad x' = -y', \quad x'' = y''$$

mit dem Modulus 1. Da somit die Reciproken von f und f_1 äquivalent sind, sind es auch f und f_1 selbst.

Alle ternären Formen der Ordnung (Ω, Δ) also, durch welche φ zur Wurzel N, N' oder zur Wurzel $-N$, $-N'$ gehörig eigentlich darstellbar ist, sind unter einander äquivalent.

Ist nun M'' eine positive oder negative Primzahl, so haben die Congruenzen (12), wenn sie überhaupt lösbar sind, nur zwei solche entgegengesetzte Wurzeln N, N'; $-N$, $-N'$, und sie sind lösbar, sobald φ durch Formen der Ordnung (Ω, Δ) eigentlich darstellbar ist. Demnach findet sich folgender Satz, welcher der gedachte Hilfssatz ist: Zwei ternäre Formen der Ordnung (Ω, Δ) sind äquivalent, wenn sie ein- und dieselbe primitive binäre Form der Determinante $-\Omega M''$ eigentlich darstellen, vorausgesetzt, dass M'' eine positive oder negative Primzahl ist, die nicht aufgeht in $2\Omega\Delta$.

4. Auf Grund dieser Hilfssätze lässt sich jetzt zunächst der folgende Satz ohne Mühe beweisen: Wenn eine unbestimmte ternäre Form, deren Invarianten Ω, Δ relativ prim sind, eine eigentlich-primitive Form ψ darstellt, deren Determinante $-\Omega M''$ prim ist zu 2Δ, so stellt sie auch jede andere binäre Form ψ_1 desselben Geschlechts dar.

Da ψ durch die unbestimmte ternäre Form darstellbar sein soll, müssen nach nr. 3 des dritten Capitels die Formen

ψ, ψ_1 entweder beide negativ oder beide unbestimmt, und werden folglich die Formen

$$\varphi = -\psi, \quad \varphi_1 = -\psi_1$$

entweder beide positiv oder beide unbestimmt sein. In dem Falle, wo dem Geschlechte der letzteren der Charakter 1 (mod. 4) zukommt und jede Ambige von demselben Charakter ist, nehmen wir zunächst an, dass die Classen von φ, φ_1 den verschiedenen Categorieen angehören, in welche die Classen dieses Geschlechts alsdann sich vertheilen. Den Bemerkungen in nr. 2 zufolge lassen sich dann zwei positive Primzahlen p, q angeben, so beschaffen, dass pq gleichzeitig durch φ und φ_1 eigentlich dargestellt wird und dass für die Fundamentalauflösung T, U der Gleichung (1) nicht $T \pm 1$ durch pq theilbar ist. Die Form φ wird mithin einer Form

$$(pq, r, s)$$

äquivalent sein, in welcher $r^2 - pq \cdot s \doteq -\Omega M''$ ist. Da nun einerseits äquivalente ternäre Formen dieselben binären Formen darstellen, andererseits äquivalente binäre Formen stets gleichzeitig darstellbar oder gleichzeitig nicht darstellbar sind, so darf man bei dem zu beweisenden Satze φ durch die Form (pq, r, s), die gegebene ternäre Form aber durch eine äquivalente Form

$$f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

ersetzen, welche die Form

$$(-pq, -r, -s)$$

als einen Bestandtheil enthält, sodass

$$a = -pq, \quad b'' = -r, \quad a' = -s,$$

also

$$b''^2 + pq \cdot a' = -\Omega M'' \tag{14}$$

ist. Heisst

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{A}, & \mathfrak{A}', & \mathfrak{A}'' \\ \mathfrak{B}, & \mathfrak{B}', & \mathfrak{B}'' \end{pmatrix}$$

ihre Reciproke, so ist

$$\mathfrak{A}'' = M''$$

und

$$\mathfrak{A}'\mathfrak{A}'' - \mathfrak{B}^2 = \Delta a = -\Delta pq. \tag{15}$$

Wenn f durch die Substitution

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & \mu \\ 0 & \nu & \varrho \end{pmatrix},$$

bei welcher

$$\lambda\varrho - \mu\nu = 1 \tag{16}$$

ist, in die äquivalente Form

$$f_1 = \begin{pmatrix} a_1, & a_1', & a_1'' \\ b_1, & b_1', & b_1'' \end{pmatrix}$$

mit der Reciproken

$$\mathfrak{F}_1 = \begin{pmatrix} \mathfrak{A}_1, & \mathfrak{A}_1', & \mathfrak{A}_1'' \\ \mathfrak{B}_1, & \mathfrak{B}_1', & \mathfrak{B}_1'' \end{pmatrix}$$

übergeht, so bestehen die Gleichungen

$$a_1 = a, \quad b_1'' = b'\nu + b''\lambda, \quad \mathfrak{A}_1'' = \mathfrak{A}''\lambda^2 - 2\mathfrak{B}\lambda\nu + \mathfrak{A}'\nu^2.$$

Nun genügen der Gleichung (16) wegen (15) die Werthe

$$\lambda = T + \mathfrak{B}U, \quad \mu = -\mathfrak{A}'U, \quad \nu = \mathfrak{A}''U, \quad \varrho = T - \mathfrak{B}U,$$

und wenn sie gewählt werden, geben die vorstehenden Gleichungen $\mathfrak{A}_1'' = \mathfrak{A}''$ d. h.

$$b_1''^2 + pq \cdot a_1' = -\Omega M'' \tag{17}$$

und

$$b_1'' \equiv b''T \pmod{pq}. \tag{18}$$

Die Gleichungen (14) und (17) lehren, dass die Congruenz

$$z^2 \equiv -\Omega M'' \pmod{pq}$$

die vier Lösungen

$$z \equiv -b'', \quad z \equiv +b'', \quad z \equiv -b_1'', \quad z \equiv +b_1''$$

besitzt; letztere sind wegen (18) und nach der Wahl der Primzahlen p, q unter einander incongruent und stellen, da die Congruenz nur vier Wurzeln besitzen kann, ihre sämmtlichen Wurzeln dar. Der Theorie der binären quadratischen Formen zufolge werden demnach die einzigen Classen von Formen mit der Determinante $-\Omega M''$, welche eigentliche Darstellungen von pq gestatten, durch die folgenden vier Formen:

$$\left(-a = pq, \ \mp b'', \ -a' = \frac{b''^2 + \Omega M''}{pq}\right),$$
$$\left(-a_1 = pq, \ \mp b_1'', \ -a_1' = \frac{b_1''^2 + \Omega M''}{pq}\right)$$

repräsentirt. Die Form φ_1, durch welche pq gleichfalls eigentlich dargestellt wird, muss daher entweder mit der ersten oder mit der dritten dieser Formen eigentlich- oder uneigentlich-äquivalent sein. Im ersten Falle ist $\psi_1 = -\varphi_1$ äquivalent mit (a, b'', a') und kann folglich dargestellt werden durch die Form f, im zweiten Falle ist sie es mit der Form

$$(a_1, b_1'', a_1')$$

und kann also dargestellt werden durch f_1, also auch wieder durch die mit f_1 äquivalente Form f, mithin in beiden Fällen durch die gegebene ternäre quadratische Form, w. z. b. w.

Die Beschränkung endlich, welche diesem Resultate in dem Falle, in welchem für das Geschlecht von φ ein Charakter 1 (mod. 4) vorhanden ist, noch anhaftet, lässt sich sogleich heben. Denn dem Bewiesenen zufolge ist jede Form $\psi_1 = -\varphi_1$, wenn φ_1 derjenigen Categorie aller Formen ihres Geschlechts, in welcher φ enthalten ist, nicht angehört, zugleich mit $\psi = -\varphi$ darstellbar, aus gleicher Erwägung nun aber wieder zugleich mit $\psi_1 = -\varphi_1$ jede Form $\psi_2 = -\varphi_2$, wenn φ_2 derselben Categorie angehört wie φ, d. h. zugleich mit $\psi = -\varphi$ jede Form desselben Geschlechts.

Man bemerke, dass durch die Formen des Geschlechts von ψ sämmtliche Primzahlen dargestellt werden können, deren quadratische Charaktere in Bezug auf die Primfaktoren von $4\Omega M''$ denjenigen gleich sind, die das Geschlecht definiren, oder welche in den diesem Geschlechte entsprechenden Linearformen

$$4\Omega M''z + \varkappa$$

enthalten sind. Somit werden alle diese Primzahlen zugleich mit ψ durch die ternäre Form darstellbar sein.

5. Seien nunmehr F und F_1 zwei unbestimmte ternäre Formen desselben Geschlechts aus der Ordnung (Ω, Δ) und Δ prim zu Ω. Nach nr. 11 des zweiten Capitels kann man eine mit F äquivalente Form

$$f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

mit der Reciproken

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{A}, & \mathfrak{A}', & \mathfrak{A}'' \\ \mathfrak{B}, & \mathfrak{B}', & \mathfrak{B}'' \end{pmatrix}$$

angeben, in welcher a prim ist gegen $2\Omega\Delta$ und $\Delta a \equiv 1$ (mod. 4), $\mathfrak{A}''$ aber ebenfalls prim gegen $2\Omega\Delta$ ist; desgleichen eine mit F_1 äquivalente Form

$$f_1 = \begin{pmatrix} a_1, & a_1', & a_1'' \\ b_1, & b_1', & b_1'' \end{pmatrix}$$

mit der Reciproken

$$\mathfrak{F}_1 = \begin{pmatrix} \mathfrak{A}_1, & \mathfrak{A}_1', & \mathfrak{A}_1'' \\ \mathfrak{B}_1, & \mathfrak{B}_1', & \mathfrak{B}_1'' \end{pmatrix},$$

in welcher a_1 prim gegen $2\Omega\Delta$ und $\Delta a_1 \equiv 1$ (mod. 4), $\mathfrak{A}_1''$ aber nicht nur zu $2\Omega\Delta$ sondern auch zu $\mathfrak{A}''$ prim ist. Da durch f die binäre Form $\psi = (a, b'', a')$, durch f_1 die binäre Form $\psi_1 = (a_1, b_1'', a_1')$ darstellbar ist, so lassen sich durch f, also auch durch F alle Primzahlen darstellen, die in gewissen, mit dem Geschlechte von ψ verträglichen arithmetischen Progressionen $4\Omega\mathfrak{A}''z + \varkappa$, durch f_1, also auch durch F_1 alle diejenigen, welche in gewissen, dem Geschlechte von ψ_1 entsprechenden Progressionen $4\Omega\mathfrak{A}_1''z + \varkappa_1$ enthalten sind. Die Charaktere von $\varkappa$ bezüglich der 4 und der Primfaktoren von $\Omega\mathfrak{A}''$ sind denjenigen von a, die Charaktere von $\varkappa_1$ bezüglich der 4 und der Primfaktoren von $\Omega\mathfrak{A}_1''$ sind denjenigen von a_1 gleich; da aber f und f_1 demselben Geschlechte ternärer Formen angehören, so ist für jeden Primfaktor ω von Ω

$$\left(\frac{a}{\omega}\right) = \left(\frac{a_1}{\omega}\right)$$

und zudem ist

$$a \equiv a_1 \pmod{4}.$$

Mithin giebt ein $\varkappa$ und ein $\varkappa_1$ nach den Primfaktoren von Ω und in Bezug auf 4 die gleichen Reste. Da ferner 4Ω prim ist gegen Δ und gegen $\mathfrak{A}'', \mathfrak{A}_1''$, sowie diese letzteren auch unter einander, so werden in den beiden Linearformen

$$4\Omega\mathfrak{A}''z + \varkappa, \quad 4\Omega\mathfrak{A}_1''z + \varkappa_1$$

gewisse gemeinsame Linearformen $4\Omega\Delta\mathfrak{A}''\mathfrak{A}_1''z + l$ enthalten

sein, deren Glieder prim zu Ω sind. Jede in den letzteren enthaltene Primzahl p wird prim sein zu $2\Omega\Delta$, der Congruenz $\Delta p \equiv 1 \pmod{4}$ genügen und sowohl durch f als durch f_1, also auch durch F und F_1 darstellbar sein. Mithin giebt es wieder zwei mit F und F_1 resp. äquivalente Formen — wir behalten der Einfachheit wegen die bisherigen Zeichen für sie bei — deren erste Coefficienten a, a_1 dieser Primzahl p gleich sind, während die aus ihren Reciproken entnommenen binären Formen

$$\Psi = (\mathfrak{A}', \mathfrak{B}, \mathfrak{A}''), \quad \Psi_1 = (\mathfrak{A}_1', \mathfrak{B}_1, \mathfrak{A}_1'')$$

(s. nr. 11 des zweiten Capitels) eigentlich primitiv sind. Diese Formen haben die gemeinsame Determinante

$$\mathfrak{B}^2 - \mathfrak{A}'\mathfrak{A}'' = \mathfrak{B}_1^2 - \mathfrak{A}_1'\mathfrak{A}_1'' = -\Delta p,$$

während $-\Delta$ die erste Invariante der Reciproken von F oder F_1 ist. Weil ferner F und F_1 demselben Geschlechte ternärer Formen angehören, muss mit Bezug auf jeden Primfaktor δ von Δ

$$\left(\frac{\mathfrak{A}''}{\delta}\right) = \left(\frac{\mathfrak{A}_1''}{\delta}\right)$$

sein, und weil p sowohl durch die Form (a, b'', a') als durch die Form (a_1, b_1'', a_1') eigentlich dargestellt wird, müssen deren Determinanten $-\Omega\mathfrak{A}''$, $-\Omega\mathfrak{A}_1'' \pmod{p}$ quadratische Reste, also

$$\left(\frac{\mathfrak{A}''}{p}\right) = \left(\frac{\mathfrak{A}_1''}{p}\right) = \left(\frac{-\Omega}{p}\right)$$

sein. Da somit alle quadratischen Charaktere der Formen Ψ, Ψ_1 nach den Primfaktoren ihrer Determinanten übereinstimmen, muss es auch der noch übrige in Bezug auf 4 vorhandene Charakter, da er durch jene mitbestimmt ist, die Formen Ψ, Ψ_1 sind also gleichen Geschlechts. Nun ist die binäre Form Ψ_1 durch die Reciproke von F_1 d. i. durch eine unbestimmte ternäre Form mit relativ primen Invarianten darstellbar; nach dem Satze der vorigen nr. ist es also auch die Form Ψ, welche aber gleichzeitig auch durch die Reciproke von F darstellbar ist. Diese beiden Reciproken gehören ebenso wie F und F_1 derselben Ordnung an; dem Hilfssatze in nr. 3 zufolge müssen sie daher und folglich auch F und

F_1 unter einander äquivalent sein. Auf solche Weise erschliesst man den Satz:

Zwei unbestimmte ternäre Formen einer Ordnung (Ω, Δ), für welche Ω, Δ relativ prim sind, gehören derselben Classe an, sobald sie desselben Geschlechts sind, oder: Jedes Geschlecht solcher unbestimmten ternären Formen besteht nur aus einer einzigen Classe*).

6. Durch diesen Satz wird die Entscheidung der Fragen, ob eine gegebene Zahl oder eine gegebene binäre Form durch eine vorgelegte primitive ternäre Form f mit der Reciproken $\mathfrak{F}$ dargestellt werden kann, für den Fall unbestimmter Formen mit relativ primen Invarianten wesentlich vereinfacht.

Handelt es sich zunächst um eine binäre Form

$$\varphi = (m, n'', m'),$$

so muss dieselbe jedenfalls die im dritten Capitel entwickelten Bedingungen der Darstellbarkeit durch irgend eine Form der Ordnung (Ω, Δ) erfüllen: 1) ihre Determinante muss von der Gestalt

$$n''^2 - mm' = -\Omega M''$$

sein, und wenn M'' prim gegen $2\Omega\Delta$ vorausgesetzt wird, muss 2) φ primitiv und darf, da f als eine unbestimmte Form angenommen wird, nicht positiv sein; 3) muss für jede in Δ aufgehende Primzahl δ die Gleichung

$$\left(\frac{M''}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right),$$

in Bezug auf jede in M'' aufgehende Primzahl p aber die Gleichung

$$\left(\frac{\varphi}{p}\right) = \left(\frac{-\Delta}{p}\right)$$

erfüllt sein. Damit aber φ durch die besondere Form f der Ordnung (Ω, Δ) darstellbar sei, muss zudem 4) für jede in Ω aufgehende Primzahl ω die Gleichung

---

*) Diesen Satz hat A. Meyer in einer kurzen Notiz (in den Schriften der Züricher Naturf. Gesellschaft XXXVII) auf quadratische Formen mit beliebig vielen Veränderlichen ausgedehnt.

$$\left(\frac{\varphi}{\omega}\right) = \left(\frac{f}{\omega}\right)$$

stattfinden. Diese Bedingungen bleiben, bis auf diejenige, dass φ primitiv sein müsse, wie leicht zu übersehen, auch bei der Annahme erforderlich, dass M'' nur prim zu 2Δ sei. Sind aber unter dieser auf M'' bezüglichen Annahme alle genannten vier Bedingungen erfüllt, so sind die in nr. 6 des dritten Capitels mit $f^{(i)}$ bezeichneten Formen sämmtlich desselben Geschlechts wie f (s. nr. 2 des sechsten Capitels), nach der vorigen nr. also sowohl unter einander als auch mit f äquivalent und demnach wird die Form φ durch die Form f eigentlich darstellbar sein.

Fragt man dagegen, ob eine gegebene Zahl m, die wir prim gegen $2\Omega\Delta$ voraussetzen wollen, eigentlich durch eine ternäre Form f der gedachten Art darstellbar sei, so kommt diese Frage nach nr. 1 des dritten Capitels auf die andere zurück, ob irgend eine binäre Form Φ der Determinante $-\Delta m$ durch die Reciproke $\mathfrak{F}$ jener Form eigentlich dargestellt werden könne. Dem eben Gefundenen gemäss sind für eine solche Form Φ die nothwendigen und hinreichenden Bedingungen dazu ausser ihrer Primitivität folgende Gleichungen:

$$(19)\qquad \left(\frac{m}{\omega}\right) = \left(\frac{f}{\omega}\right),\ \left(\frac{\Phi}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right),\ \left(\frac{\Phi}{\mu}\right) = \left(\frac{-\Omega}{\mu}\right),$$

in denen δ, ω die frühere Bedeutung haben, μ aber jeden Primfaktor von m bezeichnen soll*). Die beiden letzten Formeln schreiben der Form Φ bestimmte Geschlechtscharaktere vor; es fragt sich also nur noch, ob es eine primitive Form Φ der Determinante $-\Delta m$ giebt, welche diese Charaktere zulässt.

Dies wird offenbar der Fall sein, wenn $\Delta m \equiv 1 \pmod{4}$, denn in diesem Falle ist ein Charakter (mod. 4) vorhanden, der sich, wie auch die übrigen vorgeschrieben werden mögen, so wählen lässt, dass die Bedingung für die Existenz des Geschlechts (die Gleichung (21) des fünften Capitels) erfüllt wird.

Ist dagegen $\Delta m \equiv 3 \pmod{4}$, so entsprechen zwar, wie

*) Ist m nur prim gegen 2Ω, so werden diese Bedingungen wenigstens hinreichend sein.

im fünften Capitel nachgewiesen ist, eigentlich-primitive Formen nur der einen Hälfte aller angebbaren Gesammtcharaktere. Für eine Determinante $D = - \Delta m \equiv 1 \pmod{4}$ giebt es aber auch uneigentlich-primitive (falls $D < 0$, auch positive) Formen. Ist dann $2\mathfrak{m}$ eine, durch eine solche Form Φ darstellbare positive Zahl, wobei nach nr. 1 des fünften Capitels $\mathfrak{m}$ prim gegen $2D$ gedacht werden darf, so sind, bei leicht verständlicher Bezeichnungsweise,

$$\left(\frac{\Phi}{p}\right) = \left(\frac{2\mathfrak{m}}{p}\right), \ \left(\frac{\Phi}{p'}\right) = \left(\frac{2\mathfrak{m}}{p'}\right), \cdots \left(\frac{\Phi}{r}\right) = \left(\frac{2\mathfrak{m}}{r}\right), \cdots$$

die Einzelcharaktere der Form, und aus dem Umstande, dass D quadratischer Rest von $2\mathfrak{m}$ also auch von $\mathfrak{m}$ sein muss, fliesst, wie in nr. 4 des fünften Capitels, wenn $D = \pm P \cdot S^2$ gesetzt wird, die Dirichlet'sche Gleichung, die im vorliegenden Falle die einfachere Gestalt

$$\left(\frac{\mathfrak{m}}{P}\right) = +1$$

annimmt. Demnach sind die Einzelcharaktere der Form Φ in der Weise beschränkt, dass das Produkt derjenigen der ersten Abtheilung gleich $\left(\frac{2}{P}\right)$ also $+1$ oder -1 ist, jenachdem $\pm P \equiv 1$ oder $\pm P \equiv 5 \pmod{8}$ ist. Im letzteren Falle d. i. im Falle $\Delta m \equiv 3 \pmod{8}$ werden daher die zulässigen Combinationen der Einzelcharaktere bei den uneigentlich-primitiven Formen genau diejenigen sein, die bei den eigentlich-primitiven Formen ausgeschlossen sind, und umgekehrt. Demnach entspricht jeder beliebigen Combination der Einzelcharaktere entweder eine eigentlich- oder eine uneigentlich-primitive Form, also ist immer eine solche und zwar primitive Form Φ vorhanden, deren Charaktere die durch die Gleichungen (19) vorgeschriebenen sind. Dagegen stimmen im Falle $\Delta m \equiv 7 \pmod{8}$ die für uneigentlich-primitive Formen zulässigen Gesammtcharaktere mit den bei eigentlich-primitiven Formen zulässigen überein, und somit wird eine primitive Form Φ, deren Charaktere den durch die Gleichungen (19) vorgeschriebenen gleich sind, nur vorhanden sein, wenn letztere die Möglichkeitsbedingung erfüllen. Diese aber ist, wenn man

$$\Delta = \Delta_1 \cdot \Delta_2^2, \quad m = m_1 \cdot m_2^2$$

setzt, nämlich mit Δ_2^2, m_2^2 die grössten in Δ, m resp. aufgehenden Quadrate bezeichnet, die Gleichung

$$(20) \qquad \left(\frac{\Phi}{\Delta_1 m_1}\right) = 1,$$

welche wegen (19) die Gestalt annimmt

$$(21) \qquad \left(\frac{\mathfrak{F}}{\Delta_1}\right) = \left(\frac{-\Omega}{m_1}\right).$$

Aus diesen Betrachtungen fliesst endlich der Satz: Zur eigentlichen Darstellung der Zahl m durch die ternäre Form f ist die Bedingung

$$(22) \qquad \left(\frac{m}{\infty}\right) = \left(\frac{f}{\infty}\right)$$

nothwendig und in den Fällen

$$\Delta m \equiv 1, 3, 5 \pmod{8}$$

auch hinreichend; dagegen im Falle $\Delta m \equiv 7 \pmod{8}$ hinreichend nur in Gemeinschaft mit der Bedingung (21)*).

Betrachten wir insbesondere den Fall $\Omega = -1$. Wählt man dann $m = 1$, so wird in den Fällen $\Delta \equiv 1, 3, 5 \pmod{8}$ die Zahl 1 immer durch f darstellbar sein. Es giebt nämlich eine binäre Form $\Phi = (\mathfrak{M}', \mathfrak{N}, \mathfrak{M}'')$ mit der Determinante

$$\mathfrak{N}^2 - \mathfrak{M}'\mathfrak{M}'' = -\Delta$$

und aus einem durch die Gleichung $\left(\frac{\Phi}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right)$ bestimmten Geschlechte, welche durch $\mathfrak{F}$ eigentlich dargestellt werden kann, oder eine mit $\mathfrak{F}$ äquivalente Form

$$\mathfrak{F}_1 = \begin{pmatrix} \mathfrak{M}, & \mathfrak{M}', & \mathfrak{M}'' \\ \mathfrak{N}, & \mathfrak{N}', & \mathfrak{N}'' \end{pmatrix};$$

wird die Adjungirte der letzteren $\Delta \cdot f_1$ genannt, so ist f_1

---

*) Ist m nur prim gegen 2Ω, so ist die Bedingung (22) in Verbindung mit der anderen:

$$\left(\frac{\mathfrak{F}}{\frac{\Delta_1}{d}}\right) = \left(\frac{-\Omega}{\frac{m_1}{d}}\right),$$

welche an Stelle von (21) tritt und in welcher d den grössten gemeinsamen Theiler von Δ_1, m_1 bezeichnet, wenigstens hinreichend.

äquivalent mit f und ihr erster Coefficient ist 1, sodass man setzen darf

$$f_1 = \begin{pmatrix} 1, & m', & m'' \\ n, & n', & n'' \end{pmatrix}.$$

Diese Form ist jedoch*) einer Form

$$(23) \qquad \begin{pmatrix} 1, & a', & a'' \\ b, & 0, & 0 \end{pmatrix} \quad .$$

äquivalent, wo $a'a'' - b^2 = \Delta$, und man findet daher den Satz:

Jede ternäre Form der Ordnung $(-1, \Delta)$ ist, wenn $\Delta \equiv 1, 3, 5 \pmod{8}$, einer Form von der Gestalt (23) äquivalent.

Ist aber $\Delta \equiv 7 \pmod{8}$, so wähle man $m = -1$, sodass $\Delta m \equiv 1 \pmod{8}$ wird. Dann ist -1 durch die Form f darstellbar. Es giebt nämlich wieder eine binäre Form

$$\Phi = (\mathfrak{M}', \mathfrak{N}, \mathfrak{M}'')$$

mit der Determinante

$$\mathfrak{N}^2 - \mathfrak{M}'\mathfrak{M}'' = \Delta$$

und aus einem durch die Gleichung $\left(\frac{\Phi}{\delta}\right) = \left(\frac{\mathfrak{F}}{\delta}\right)$ bestimmten Geschlechte, welche durch $\mathfrak{F}$ dargestellt werden kann, und man findet wie im vorigen Falle den Satz: Jede ternäre Form der Ordnung $(-1, \Delta)$ ist, wenn $\Delta \equiv 7 \pmod{8}$, einer Form von der Gestalt

$$(24) \qquad \begin{pmatrix} -1, & a', & a'' \\ b, & 0, & 0 \end{pmatrix}$$

äquivalent, wo $b^2 - a'a'' = \Delta$ ist.

7. Von den in der vorigen nr. erhaltenen Resultaten sollen nun ein paar interessante Anwendungen gemacht werden.

Im vierten Capitel ist die Aufstellung der ganzzahligen Transformationen einer unbestimmten ternären Form f in sich selbst für den Fall, dass die Determinante der letzteren keine quadratischen Faktoren hat, auf die Auflösung gewisser Gleichungen von der Form

*) Die Richtigkeit dieser Behauptung ergiebt sich durch die Reduktion der Form und wird im dritten Abschnitte bewiesen werden.

$$(25) \qquad p^2 + F(q, q', q'') = 2^\lambda \varDelta_0$$

in ganzen Zahlen p, q, q', q'', deren erste durch $\varDelta_0$ theilbar ist, zurückgeführt worden. Es wurde dort bereits die Frage aufgeworfen, ob alle diese Gleichungen wirklich solche ganzzahligen Lösungen besitzen? Die gewonnenen Sätze verstatten jetzt, diese Frage zu erörtern und zu bejahen.

Da die Invarianten der Form f nach der Voraussetzung $-1, \varDelta$ sind, ist sie einer Form entweder von der Gestalt (23) oder von der Gestalt (24) äquivalent.

Mit Rücksicht darauf, dass die Betrachtungen ganz dieselben bleiben, welcher dieser Fälle Statt hat, dürfen wir uns auf die Erörterung des ersteren beschränken. Weil die Adjungirte von (23) die Form

$$\begin{pmatrix} a'a'' - b^2, & a'', & a' \\ -b, & 0, & 0 \end{pmatrix}$$

ist, können a', b, a'' keinen gemeinsamen Theiler haben. Daher darf man a' als prim gegen $\varDelta$, b und folglich a'' durch $\varDelta_0$ theilbar voraussetzen; denn, ist das erstere noch nicht der Fall, so lässt sich doch durch (a', b, a'') eine gegen $\varDelta$ prime Zahl darstellen und die Form (23) durch eine, nur die beiden Veränderlichen x', x'' betreffende Substitution in eine andere derselben Gestalt überführen, in welcher a' durch diese Zahl ersetzt ist. Darauf geht diese durch die Substitution

$$x = y, \quad x' = y' + \beta y'', \quad x'' = y''$$

in eine äquivalente über, in welcher b durch $b + a'\beta$ ersetzt, also bei geeigneter Wahl von β durch $\varDelta_0$ theilbar ist. Nennen wir die so beschaffene, mit f äquivalente Form

$$f_1 = \begin{pmatrix} 1, & a', & a_1''\varDelta_0 \\ b_1\varDelta_0, & 0, & 0 \end{pmatrix},$$

so ist

$$F_1 = \begin{pmatrix} \varDelta, & a_1''\varDelta_0, & a' \\ -b_1\varDelta_0, & 0, & 0 \end{pmatrix}$$

ihre Adjungirte. Diese aber stellt genau dieselben Zahlen dar, wie die Form F und daher wird die Gleichung (25) gleichzeitig mit der folgenden:

$$p^2 + F_1(q, q', q'') = 2^\lambda \Delta_0$$

d. i. mit

$$p^2 + \Delta q^2 + a_1'' \Delta_0 q'^2 + a' q''^2 - 2 b_1 \Delta_0 q' q'' = 2^\lambda \Delta_0$$

auflösbar resp. nicht auflösbar sein. Da p durch Δ_0 theilbar zu denken ist, lehrt diese Gleichung, dass es auch q'' sein muss, und wenn demgemäss

$$p = \Delta_0 r, \; q = s, \; q' = s', \; q'' = \Delta_0 s'', \; \Delta = \Delta_0 \Delta_1$$

sowie

$$2^\lambda - \Delta_0 r^2 = m$$

gesetzt wird, nimmt sie folgende Gestalt an:

$$\Delta_1 s^2 + a_1'' s'^2 + a' \Delta_0 s''^2 - 2 b_1 \Delta_0 s' s'' = m, \tag{26}$$

mithin ist nur die Frage, ob die Zahl r so gewählt werden kann, dass die Zahl m durch die ternäre Form

$$f_2 = \begin{pmatrix} \Delta_1, & a_1'', & a'\Delta_0 \\ -b_1\Delta_0, & 0, & 0 \end{pmatrix}$$

darstellbar ist. Aus der Identität

$$\Delta_0(\Delta x^2 + a_1'' \Delta_0 x'^2 + a' x''^2 - 2 b_1 \Delta_0 x' x'')$$
$$= \Delta_1 (\Delta_0 x)^2 + a_1'' (\Delta_0 x')^2 + a' \Delta_0 x''^2 - 2 b_1 \Delta_0 (\Delta_0 x') x''$$

ersieht man zuerst, dass letztere Form zugleich mit F_1 oder f_1 eine unbestimmte Form ist. Ihre Determinante findet sich gleich $\Delta_1^2 \cdot \Delta_0$*), ihre Adjungirte gleich Δ_1 mal der Form

$$\begin{pmatrix} \Delta_0, & a'\Delta_0, & a_1'' \\ b_1\Delta_0, & 0, & 0 \end{pmatrix};$$

da Δ also auch Δ_0 keine quadratischen Theiler hat, mithin Δ_0, Δ_1 relativ prim sind, muss letztere Form primitiv, mithin die Invarianten von f_2 gleich $-\Delta_1, \Delta_0$ sein. Jedenfalls wird daher zur Darstellbarkeit von m mit Bezug auf jeden Primfaktor δ_1 von Δ_1 die Bedingung

$$\left(\frac{m}{\delta_1}\right) = \left(\frac{f_2}{\delta_1}\right) \tag{27}$$

---

*) Diese Determinante kann negativ sein, da Δ_0 irgend einen positiven oder negativen Theiler von Δ bezeichnet; um in diesem Falle die obigen Sätze anwenden zu können, hätte man nur statt der Darstellbarkeit von m durch f_2 diejenige von $-m$ durch $-f_2$ zu betrachten.

erforderlich sein, wenn anders nicht m durch δ_1 theilbar ist. Das Letztere könnte sich nur ereignen, wenn δ_1 einer derjenigen Primfaktoren δ_1' ist, in Bezug auf welche $2^\lambda \Delta_0$ quadratischer Rest ist, und ist in jedem solchen Falle durch zwei bezügliche Reste der Zahl r und zwar in der Weise zu erreichen, dass m durch δ_1' aber nicht durch $\delta_1'^2$ theilbar wird; man darf daher, indem man das Produkt der Primfaktoren δ_1' mit d' bezeichnet, $m = m'd'$ voraussetzen, wo nun m' prim ist gegen d'. Für jeden derjenigen Primfaktoren $\delta_1 = \delta_1''$ aber, in Bezug auf welche $2^\lambda \Delta_0$ quadratischer Nichtrest ist, lässt sich der bezügliche Rest von r so wählen, dass m die Bedingung (27) erfüllt; denn, indem man r alle δ_1'' Reste durchlaufen lässt, nimmt dieser Ausdruck $\frac{\delta_1''+1}{2}$ nicht durch δ_1'' theilbare Reste an, unter denen mindestens ein quadratischer Rest und ein Nichtrest vorhanden sein muss. Diesen Bestimmungen gemäss wird offenbar m prim sein gegen d'', wenn d'' das Produkt aller Primfaktoren δ_1'' bezeichnet; und folglich wird m' prim sein gegen d'' und d', also gegen Δ_1. Endlich wähle man den Rest von r (mod. $4\Delta_0$), was mit allen bisherigen Bestimmungen verträglich ist, so, dass m prim gegen Δ_0, und $\Delta_0 m$ einer der Zahlen 1, 5 (mod. 8) congruent wird. Alsdann wird m in der That durch die Form f_2 darstellbar sein.

Um sich hiervon zu überzeugen, darf man wieder f_2 durch eine äquivalente Form ersetzen und deshalb, ähnlich wie bei f_1, voraussetzen, dass b_1 und a_1'' durch d' theilbar sind. Dann erfordert die Gleichung (26), dass auch s'' durch d' theilbar sei, und ist, wenn demgemäss darin $d's''$ an Stelle von s'' und $a_1'' = d'a_2''$ gesetzt wird, zugleich auflösbar oder nicht auflösbar mit der Gleichung

$$(28)\qquad d''s^2 + a_2''s'^2 + a'\Delta_0 d's''^2 - 2b_1\Delta_0 s's'' = m'.$$

Nun ist nach der Identität

$$(29)\quad \begin{cases} d'(d''x^2 + a_2''x'^2 + a'\Delta_0 d'x''^2 - 2b_1\Delta_0 x'x'') \\ \qquad = \Delta_1 x^2 + a_1''x'^2 + a'\Delta_0(d'x'')^2 - 2b_1\Delta_0 x'(d'x'') \end{cases}$$

die Form

$$f_3 = \begin{pmatrix} d'', & a_2'', & a'\Delta_0 d' \\ -b_1\Delta_0, & 0, & 0 \end{pmatrix}$$

wieder zugleich mit f_2 eine unbestimmte Form, ihre Determinante gleich $d''^2 \cdot d'\Delta_0$, ihre Adjungirte gleich d'' mal der Form

$$\begin{pmatrix} d'\Delta_0, & a'\Delta_0 d', & a_2'' \\ b_1\Delta_0, & 0, & 0 \end{pmatrix},$$

welche primitiv ist, da $d'\Delta_0$ keinen quadratischen Theiler hat und prim ist gegen d''; demnach sind die Invarianten von f_3 gleich $\pm d''$, $d'\Delta_0$ also relativ prim. Aus den Gleichungen (27) und (29) folgen aber mit Bezug auf jeden Primfaktor δ_1'' der Invariante d'' die Gleichungen

$$\left(\frac{d'm'}{\delta_1''}\right) = \left(\frac{f_2}{\delta_1''}\right), \quad \left(\frac{d'f_3}{\delta_1''}\right) = \left(\frac{f_2}{\delta_1''}\right)$$

mithin auch

$$\left(\frac{m'}{\delta_1''}\right) = \left(\frac{f_3}{\delta_1''}\right);$$

zudem ist m' ungerade und prim sowohl gegen Δ_0 als gegen Δ_1 und somit auch gegen $2d'' \cdot d'\Delta_0$, und endlich ist

$$\Delta_0 m \text{ d. i. } d'\Delta_0 \cdot m' \equiv 1 \text{ oder } 5 \pmod{8}.$$

In Folge dieser Umstände ist nach dem allgemeinen Satze der vorigen nr. m' eigentlich durch die Form f_3 darstellbar, also hat die Gleichung (28) und in Folge davon auch die Gleichung (26) eine Auflösung und die in Rede stehende Gleichung (25):

$$p^2 + F(q, q', q'') = 2^\lambda \Delta_0$$

ist in der Weise auflösbar, dass p theilbar wird durch Δ_0, w. z. b. w. —

8. Eine weitere Anwendung können wir von dem Satze in nr. 6 machen, um die Bedingungen festzustellen, unter welchen die Gleichung*)

$$(30) \qquad ax^2 + by^2 + cz^2 + du^2 = 0$$

ganzzahlige Auflösungen gestattet. Der Einfachheit wegen beschränken wir uns jedoch auch hier auf den Fall, wo die quaternäre Form eine ungerade Determinante hat,

*) S. zu dieser und der folgenden nr. A. Meyer, Mathematische Mittheilungen, Züricher naturf. Ges. v. J. 1883.

a, b, c, d also ungerade Zahlen bedeuten. Die Zahlen x, y, z, u dürfen ohne einen von 1 verschiedenen gemeinsamen Theiler vorausgesetzt werden. Das Gleiche gilt von den vier Coefficienten; zudem darf man letztere ohne quadratische Theiler annehmen; denn wären

$$a = a'p^2, \quad b = b'q^2, \quad c = c'r^2, \quad d = d's^2$$

und p^2, q^2, r^2, s^2 die grössten in a, b, c, d enthaltenen Quadrate, so flösse aus jeder ganzzahligen Auflösung der Gleichung (30) eine eben solche Auflösung

$$x' = px, \quad y' = qy, \quad z' = rz, \quad u' = su$$

der Gleichung

$$(31) \qquad a'x'^2 + b'y'^2 + c'z'^2 + d'u'^2 = 0$$

und aus einer ganzzahligen Lösung der letzteren, indem man diese mit $p^2 q^2 r^2 s^2$ multiplicirt, eine ebensolche Auflösung

$$x = qrsx', \quad y = prsy', \quad z = pqsz', \quad u = pqru'$$

der Gleichung (30), sodass die Gleichungen (30) und (31) zugleich auflösbar und zugleich nicht auflösbar sind. Ferner dürfen auch je drei der Coefficienten ohne einen gemeinsamen Theiler gedacht werden; denn hätten etwa a, b, c den Primtheiler p gemeinsam, sodass

$$a = pa', \quad b = pb', \quad c = pc'$$

wäre, so müsste dieser, da d nicht durch ihn aufgeht, ein Theiler von u, $u = pu'$ sein, die Gleichung (30) wäre gleichzeitig lösbar oder nicht lösbar mit der Gleichung

$$a'x^2 + b'y^2 + c'z^2 + dp \cdot u'^2 = 0,$$

in welcher das Produkt aller Coefficienten

$$a'b'c' \cdot dp = \frac{abcd}{p^2} < abcd$$

wäre; da also beim Fortgange dieser Betrachtung das Produkt der Coefficienten jedesmal verringert wird, muss man endlich auf eine Gleichung kommen, welche mit (30) gleichzeitig lösbar resp. nicht lösbar ist, und in welcher die gedachte Annahme zutrifft. Demgemäss machen wir sie für die vorgelegte Gleichung (30). Bezeichnet man den grössten gemeinsamen positiven Theiler zweier Zahlen m, n mit (mn), sodass

$$(mn) = (nm)$$

ist, so darf man dann setzen

$$\begin{aligned} a &= (ab)(ac)(ad) \cdot \alpha \\ b &= (ba)(bc)(bd) \cdot \beta \\ c &= (ca)(cb)(cd) \cdot \gamma \\ d &= (da)(db)(dc) \cdot \delta, \end{aligned}$$

wo die Zahlen

$$(ab),\ (ac),\ (ad),\ (bc),\ (bd),\ (cd),\ \alpha,\ \beta,\ \gamma,\ \delta$$

zu je zweien relativ prim sein müssen.

Betrachten wir nun die sechs Produkte

$$(32) \qquad -ab,\ -ac,\ -ad,\ -bc,\ -bd,\ -cd$$

und sei p irgend eine der nur in endlicher Anzahl vorhandenen Primzahlen, welche in $abcd$ aufgehen. Diese kann höchstens in zwei der vier Zahlen a, b, c, d aufgehen; thut sie das z. B. in a, b, so ist $-cd$ das einzige der Produkte (32), das nicht durch p theilbar ist, und wenn die Gleichung (30) stattfinden soll, so muss

$$cz^2 + du^2 \equiv 0 \pmod{p}$$

also entweder $-cd$ quadratischer Rest von p, entgegengesetzten Falls z, u theilbar durch p,

$$z = pz', \quad u = pu'$$

sein; und wenn man noch $a = pa'$, $b = pb'$ setzt, so ist in diesem Falle die Gleichung (30) gleichzeitig lösbar oder nicht lösbar mit der folgenden:

$$(33) \qquad a'x^2 + b'y^2 + cp \cdot z'^2 + dp \cdot u'^2 = 0,$$

in welcher weder x noch y durch p theilbar sein kann, da sonst entweder x, y, z, u diesen Faktor gemeinsam, oder b resp. a den quadratischen Theiler p^2 haben würden. Von den, der letzteren Gleichung entsprechenden Produkten

$$(34) \qquad \begin{cases} -a'b', \ -a'cp = -ac, \ -a'dp = -ad, \\ -b'cp = -bc, \ -b'dp = -bd, \ -cdp^2 \end{cases}$$

ist nur das erste nicht theilbar durch p und aus (33) ergiebt sich $-a'b'$ als quadratischer Rest von p; in Bezug auf jede andere Primzahl aber verhalten sich die Produkte sei es in

Betreff der Theilbarkeit oder in Betreff ihres quadratischen Charakters genau, wie die entsprechenden Produkte (32), da sie ihnen theils gleich, theils nur durch den Faktor p^2 von ihnen verschieden sind. Man ersieht aus diesen Gründen, dass es möglich sein muss, die Gleichung (30), falls sie Lösungen gestattet, durch eine andere zu ersetzen, deren Coefficienten, ohne dass sie aufhören, den früheren Voraussetzungen zu entsprechen, so beschaffen sind, dass in Bezug auf jede Primzahl, die zweien von ihnen gemeinsam ist, das negativ genommene Produkt der beiden anderen quadratischer Rest ist.

Hieraus aber ergiebt sich unmittelbar, dass die folgenden Bedingungen zur Auflösbarkeit der Gleichung (30) erforderlich sind:

1) $-(ac)(ad)(bc)(bd)\gamma\delta$ quadrat. Rest von (ab)
$-(ab)(ad)(cb)(cd)\beta\delta$ „ „ „ (ac)
$-(ab)(ac)(db)(dc)\beta\gamma$ „ „ „ (ad)
$-(ba)(bd)(ca)(cd)\alpha\delta$ „ „ „ (bc)
$-(ba)(bc)(da)(dc)\alpha\gamma$ „ „ „ (bd)
$-(ca)(cb)(da)(db)\alpha\beta$ „ „ „ (cd)

2) dürfen, was kaum bemerkt zu werden braucht, a, b, c, d nicht sämmtlich gleichen Vorzeichens sein; demgemäss darf man, indem man eventuell die Gleichung mit entgegengesetztem Zeichen schreibt, etwa a, b positiv, c negativ voraussetzen, während d positiv oder negativ sein kann.

Man bemerke ferner, dass aus der Gleichung (30) auch die Congruenz folgt:

$$ax^2 + by^2 + cz^2 + du^2 \equiv 0 \pmod{8}.$$

Da aber x, y, z, u nicht gleichzeitig gerade sein dürfen, können sie nur entweder sämmtlich ungerade, oder zwei von ihnen, etwa x, y ungerade, die beiden anderen gerade sein. Im ersten Falle müsste

$$a + b + c + d \equiv 0 \pmod{8}$$

sein; im zweiten folgt $a + b \equiv 0 \pmod{4}$ also

entweder

$$a + b \equiv 0 \quad \text{d. i.} \quad ab \equiv -1 \pmod{8}$$

oder

$$a + b \equiv 4 \quad \text{d. i.} \quad ab \equiv 3 \pmod{8}.$$

Ist nun

$$abcd \equiv 1 \pmod{8},$$

so folgt im ersteren Falle

$$cd \equiv -1, \quad \text{d. i.} \quad c + d \equiv 0$$

im zweiten Falle

$$cd \equiv 3, \quad \text{d. i.} \quad c + d \equiv 4 \quad \Bigg\} \pmod{8}$$

also in beiden Fällen

$$a + b + c + d \equiv 0 \pmod{8}.$$

Man hat also alsdann den obigen zwei Bedingungen noch folgende dritte als erforderlich hinzuzufügen:

3) Ist

$$abcd \equiv 1 \pmod{8},$$

so muss

$$a + b + c + d \equiv 0 \pmod{8}$$

sein.

Es soll nun gezeigt werden, dass, wenn diese nothwendigen Bedingungen erfüllt sind, die Gleichung (30) lösbar ist d. h. dass alsdann bei passender Wahl von u die Zahl

$$m = du^2$$

durch die unbestimmte, primitive ternäre Form

$$f = -ax^2 - by^2 - cz^2$$

dargestellt werden kann. Dies folgt aber in der That für $u = 1$ aus den Sätzen der nr. 6. Die Invarianten der Form f sind nämlich durch die Gleichungen

$$\Omega = -(ab)(bc)(ca), \quad \Delta = -(ad)(bd)(cd)\alpha\beta\gamma$$

bestimmt, also relativ prim, sowie ohne quadratische Theiler, während

$$m = d = (ad)(bd)(cd)\delta$$

ebenfalls ohne quadratische Theiler ist.

Wenn daher $\Delta d \equiv 1, 3, 5 \pmod{8}$ ist, so ist zur Darstellbarkeit von m durch die Form f das Bestehen der Gleichung

$$(35)\qquad \left(\frac{f}{\omega}\right) = \left(\frac{m}{\omega}\right) = \left(\frac{d}{\omega}\right)$$

für jeden Primfaktor ω von Ω hinreichend. Wenn nun zuerst ω ein Primfaktor von (ab) ist, so hat man

$$\left(\frac{f}{\omega}\right) = \left(\frac{-c}{\omega}\right) = \left(\frac{-(ca)(cb)(cd)\gamma}{\omega}\right)$$

$$\left(\frac{d}{\omega}\right) = \left(\frac{(ad)(bd)(cd)\delta}{\omega}\right)$$

also

$$\left(\frac{df}{\omega}\right) = \left(\frac{-(ac)(ad)(bc)(bd)\gamma\delta}{\omega}\right)$$

d. i. nach der ersten der unter 1) vorausgesetzten Gleichungen

$$\left(\frac{df}{\omega}\right) = 1.$$

Ebenso bestätigt sich die Gleichung (35) für jeden der übrigen Primfaktoren von Ω und somit sind die unter 1) und 2) gemachten nothwendigen Voraussetzungen zur Lösbarkeit der Gleichung (30) auch ausreichend.

Wenn dagegen $\Delta d \equiv 7 \pmod{8}$ oder, was dasselbe sagt,

$$\alpha\beta\gamma\delta \equiv abcd \equiv 1 \pmod{8}$$

ist, so reicht zur Darstellbarkeit der Zahl $m = d$ durch die Form f die Gleichung (35) nur in Gemeinschaft mit der anderen Gleichung

$$(36)\qquad \left(\frac{\mathfrak{F}}{\alpha\beta\gamma}\right) = \left(\frac{-\Omega}{\delta}\right)$$

aus, die hier an Stelle der Bedingungsgleichung (21) tritt und in welcher $\mathfrak{F}$ die Reciproke von f, nämlich die Form

$$-(bc)(cd)(db)\beta\gamma\cdot x^2 - (ca)(ad)(dc)\gamma\alpha\cdot y^2 - (ab)(bd)(da)\alpha\beta\cdot z^2$$

vorstellt. Während nun die Gleichung (35) wieder zugleich mit den Voraussetzungen unter 1) erfüllt wird, findet die Gleichung (36) statt, sobald die in diesem Falle noch erforderliche Voraussetzung 3) erfüllt ist. Dieser Gleichung kann nämlich folgende Gestalt:

$$\left(\frac{-(bc)(cd)(db)\beta\gamma}{\alpha}\right)\cdot\left(\frac{-(ca)(ad)(dc)\gamma\alpha}{\beta}\right)\cdot\left(\frac{-(ab)(bd)(da)\alpha\beta}{\gamma}\right)$$
$$\cdot\left(\frac{(ab)(bc)(ca)}{\delta}\right) = 1$$

oder auch mittels des Reciprocitätsgesetzes diese andere:

$$(-1)^{\frac{\alpha+\beta+\gamma+\delta}{4}} \cdot \left(\frac{(bc)(cd)(db)}{\alpha}\right) \cdot \left(\frac{(ca)(ad)(dc)}{\beta}\right) \cdot \left(\frac{(ab)(bd)(da)}{\gamma}\right) \cdot \left(\frac{(ab)(bc)(ca)}{\delta}\right) = 1$$

gegeben werden. Eine weitere Umformung der linken Seite*) mittels des Reciprocitätsgesetzes giebt unter Rücksicht auf die Congruenz

$$\alpha\beta\gamma\delta \equiv 1 \pmod{8}$$

statt der letzten Gleichung die neue:

$$(37) \qquad (-1)^{\frac{\sigma}{4}} = 1,$$

in welcher, wenn zur Abkürzung

$$\begin{aligned} \Sigma_1 &= (ab) + (ac) + (ad) + (bc) + (bd) + (cd) \\ \Sigma_2 &= (ab)(ac) + (ab)(ad) + (ab)(bc) + (ab)(bd) \\ &+ (ac)(ad) + (ac)(bc) + (ac)(cd) + (ad)(bd) \\ &+ (ad)(cd) + (bc)(bd) + (bc)(cd) + (bd)(cd) \end{aligned}$$

gesetzt wird

$$\sigma \equiv (a+b+c+d)[(ab)(cd)+(ac)(bd)+(ad)(bc)] - 4(\Sigma_2 - 2\Sigma_1) \pmod{8}$$

ist. Nun ist Σ_2 als Summe von zwölf ungeraden Zahlen eine gerade Zahl, also einfacher

$$\sigma \equiv (a+b+c+d)[(ab)(cd)+(ac)(bd)+(ad)(bc)] \pmod{8}.$$

Ist demnach die Bedingung 3) erfüllt, so ist

$$\sigma \equiv 0 \pmod{8}$$

mithin auch die Gleichung (37) d. i. die Gleichung (36) erfüllt, also die Gleichung (30) auflösbar.

Auf solche Weise ist der Satz festgestellt: Zur Auflösbarkeit der Gleichung (30) mit ungeraden Coefficienten sind, wenn

$$abcd \equiv 3, 5, 7 \pmod{8}$$

ist, die Bedingungen unter 1) und 2), wenn aber

*) S. die angeführte Arbeit S. 214 u. ff.

$$abcd \equiv 1 \pmod{8}$$

ist, diese Bedingungen gemeinsam mit der Bedingung 3) nothwendig und hinreichend.

Man findet in Meyer's Abhandlung die Bedingungen auch für den Fall, dass a, b, c, d nicht sämmtlich ungerade sind, sowie allgemeiner die Bedingungen dafür angegeben, dass irgend eine quaternäre Form den Werth Null darstelle; hier kann darauf nur verwiesen werden.

9. Auf ähnliche Weise aber überzeugt man sich davon, dass die Gleichung

$$ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0 \tag{38}$$

mit ungeraden Coefficienten jederzeit Auflösungen gestattet, wenn diese Coefficienten nicht sämmtlich gleichen Vorzeichens sind.

Zunächst braucht man nur Auflösungen in Zahlen x, y, z, u, v ohne einen von 1 verschiedenen gemeinsamen Theiler in Betracht zu ziehen; auch darf man die Coefficienten ohne einen solchen gemeinsamen und gleichfalls ohne einen quadratischen Theiler voraussetzen. Es ist auch wieder zulässig anzunehmen, dass je drei der Coefficienten ohne einen gemeinsamen Theiler sind; denn hätten z. B. a, b, c einen gemeinsamen Primtheiler p, so setze man

$$a = pa', \quad b = pb', \quad c = pc'$$

und gleichzeitig $u = pu'$, $v = pv'$. Ist dann die Gleichung

$$a'x^2 + b'y^2 + c'z^2 + dp \cdot u'^2 + ep \cdot v'^2 = 0$$

auflösbar, so wird es offenbar die gegebene ebenfalls sein. Nun ist die Determinante der neuen quinären Form

$$a'b'c' \cdot dp \cdot ep = \frac{abcde}{p}$$

also kleiner als diejenige der ursprünglichen; indem man also in gleicher Weise, wenn nöthig, fortfährt, muss man endlich zu einer Gleichung derselben Form wie (38) gelangen, deren Coefficienten die gemachten Voraussetzungen erfüllen und deren Lösbarkeit zugleich auch die Lösbarkeit der ersteren verbürgt. Machen wir daher diese Annahme von vornherein bei der Gleichung (38).

Zu ihrer Auflösbarkeit ist dann jedenfalls erforderlich, dass nicht alle Coefficienten gleiches Vorzeichen haben. Man darf also etwa a, b positiv, c negativ annehmen und dann kommt die Behauptung darauf hinaus, dass, falls die ausgesprochene nothwendige Bedingung erfüllt ist, bei geeigneten Werthen von u, v die Zahl

$$m = du^2 + ev^2$$

durch die unbestimmte, primitive ternäre Form

$$f = -ax^2 - by^2 - cz^2$$

dargestellt werden kann. Nun darf man setzen

$$\begin{aligned} a &= (ab)(ac) \cdot \alpha \\ b &= (ba)(bc) \cdot \beta \\ c &= (ca)(cb) \cdot \gamma \\ d = (de) \cdot \delta, &\quad e = (ed) \cdot \varepsilon, \end{aligned}$$

wo nach den gemachten Annahmen die Zahlen

$$(ab),\ (ac),\ (bc),\ \alpha,\ \beta,\ \gamma$$

zu je zweien und auch zu $(de) = (ed)$ prim sind. Als Invarianten von f ergeben sich

$$\Omega = -(ab)(bc)(ca), \quad \Delta = -\alpha\beta\gamma,$$

und da (de) prim ist gegen $2\Omega\Delta$ und die binäre Form

$$\varphi = \delta u^2 + \varepsilon v^2$$

eigentlich primitiv ist, kann man u, v so wählen, dass die Zahl m prim zu $2\Omega\Delta$ wird, und zudem so, dass die Congruenz $\Delta m \equiv 7 \pmod{8}$ nicht statt hat. Den Sätzen in nr. 6 zufolge ist alsdann die Darstellung einer solchen Zahl m durch f stets möglich, wenn für jeden Primfaktor ω von Ω die Gleichung

$$\left(\frac{f}{\omega}\right) = \left(\frac{m}{\omega}\right) = \left(\frac{(de)\cdot\varphi}{\omega}\right)$$

oder

$$\left(\frac{\varphi}{\omega}\right) = \left(\frac{(de)\cdot f}{\omega}\right)$$

erfüllt ist. Da jedoch die Determinante $-\delta\varepsilon$ der Form φ zu Ω prim ist, so lassen ihre Geschlechtscharaktere es zu, diesen Bedingungen zu genügen, und folglich ergiebt sich die

Darstellbarkeit der Zahl m durch die Form f und die Auflösbarkeit der Gleichung (38).

Uebrigens ist diese Gleichung auch auflösbar, wenn die Coefficienten nicht sämmtlich ungerade, sondern nur vorausgesetzt wird, dass sie verschiedenen Vorzeichens sind; allgemeiner kann die Null durch jede quadratische Form mit fünf, demnach auch durch jede solche mit mehr als fünf Veränderlichen dargestellt werden, wenn diese nur keine bestimmte Form ist; s. darüber den zweiten Abschnitt, Cap. 8, Ende. —

10. In einer weiteren Reihe von Abhandlungen hat A. Meyer seine Untersuchungen auf allgemeinere Geschlechter ternärer quadratischer Formen ausgedehnt. Leider erfordern dieselben einen ausserordentlich complicirten Apparat sehr umständlicher Detailbetrachtungen, die der genannte Forscher mit bewundernswerther Energie und Unerschrockenheit durchführt, welche indessen nur schwer durchsichtig sind und so die Vermuthung begründen, dass der eingeschlagene Weg nicht eben der sachgemässeste sei, vielmehr ein anderer zu finden sein werde, welcher, mehr den inneren Gründen der Frage entsprungen, klarere Einsicht gewährt und einfacher zum Ziele führt. Die Bedeutung, welche diesen Arbeiten Meyer's ohne Frage zukommt, kann durch solche Bemerkung nicht geschmälert werden. Aber ihre bezeichnete Beschaffenheit macht es ganz unmöglich, hier auch nur eine einigermassen genügende, leicht verständliche Skizze von ihnen zu entwerfen; wir müssen uns damit begnügen, den Gang anzudeuten, den die Untersuchung nimmt, und ihre Hauptresultate zu bemerken.

Im 98. Bande des Journ. f. d. Mathematik sucht Meyer zunächst die Classenanzahl jedes ternären Nullgeschlechts d. h. jedes Geschlechts ternärer Formen, durch welche die Null darstellbar ist, für beliebige ungerade Invarianten Ω, Δ.

Nachdem er dieselbe für solche ungerade Invarianten Ω, Δ, welche gewissen einfachen Voraussetzungen genügen, mittels reducirter Formen von besonderer Gestalt gefunden hat — wo dann z. B., falls der grösste gemeinsame Theiler derselben nur Primfaktoren von der Form $4n+3$ enthält, jedes Nullgeschlecht nur aus einer Classe besteht, allgemein

aber die Anzahl der Classen eine Potenz von Zwei ist (s. nr. 5 daselbst) — verwendet er, um von solchen Invarianten zu irgend welchen ungeraden überzugehen, das von uns im siebenten Capitel auseinandergesetzte Eisenstein'sche Princip der Transformation einer ternären Form mit der Determinante D in eine solche, deren Determinante ein vorgeschriebenes Vielfaches von D ist. Jede primitive Nullform mit den Invarianten $\Omega, \Delta p^2$ (wo p eine Primzahl) entsteht nämlich aus einer solchen mit den Invarianten Ω, Δ durch eine Substitution mit dem Modulus p (nr. 9 daselbst). Um die nicht äquivalenten zu erhalten, hat man (nr. 10 daselbst) nur aus jeder Classe von Nullformen mit den Invarianten Ω, Δ eine beliebige Form herauszugreifen, auf jede so erhaltene Form sämmtliche reducirte Substitutionen vom Modulus p anzuwenden, darauf von den so entstehenden Formen diejenigen, welche nicht primitiv sind oder nicht die Invarianten $\Omega, \Delta p^2$ haben, wegzuwerfen und von den übrigen nur nicht-äquivalente Formen beizubehalten, wobei zu bemerken ist, dass nicht-äquivalente Formen mit den Invarianten Ω, Δ niemals äquivalente Formen mit den Invarianten $\Omega, \Delta p^2$ liefern können (nr. 29 daselbst). Die primitiven Formen mit den Invarianten $\Omega, \Delta p^2$, welche so entstehen können, werden aufgestellt, und nun ist die Haupt-Aufgabe und -Schwierigkeit die: über die Aequivalenz derselben zu entscheiden und die Anzahl der Classen zu erkennen, in welche sie zerfallen. Hier tritt vornehmlich die bemerkte Complikation der Betrachtungen ein; ein dabei vorgekommenes Versehen merkt Meyer selbst im Journ. f. d. Math. 112 S. 88 an. Die Diskussion führt zu dem Ergebnisse, dass, wenn die Classenanzahl in jedem Nullgeschlechte mit den Invarianten Ω, Δ eine Potenz von Zwei sei, sie es auch in jedem Nullgeschlechte mit den Invarianten $\Omega, \Delta p^2$ sein müsse (nr. 28 daselbst).

Ausgehend von dem anfangs mitgetheilten einfachen Falle leitet Meyer dann vermittelst dieser Erkenntniss als Resultat des Ganzen den Satz her, dass in jedem Nullgeschlechte mit ungeraden Invarianten Ω, Δ die Anzahl der Classen eine Potenz von Zwei sei, welche er näher determinirt (nr. 30 daselbst, besser J. f. Math. 112 S. 87).

In seiner letzten Arbeit, welche durch die Bände 113—116 des J. f. Math. sich hindurchzieht, erweitert Meyer diese Untersuchungen über Nullformen auf beliebige unbestimmte ternäre quadratische Formen mit ungerader Determinante. Das Princip seiner Untersuchung und demgemäss auch ihr allgemeiner Gang bleiben genau dieselben wie zuvor. Aber die Verkettung der verschiedenen Sätze und Theorieen, deren die Untersuchung bedarf, wird noch bei weitem complicirter, die Details der Diskussionen noch weit erdrückender als dort, sodass wir genöthigt sind, den Leser, welcher ein Interesse dafür findet, auf die genannte Arbeit selbst zu verweisen, und hier nur Kenntniss geben können von dem Satze, welchen Meyer als Endergebniss seiner Untersuchung ausspricht. Er lautet (J. f. Math. 116 S. 317) folgendermassen:

Ist Θ der grösste gemeinsame Theiler von Ω und Δ und sind Ω_2^2, Δ_2^2 die grössten in Ω, Δ aufgehenden Quadrate:

$$\Omega = \Omega_1 \Omega_2^2, \quad \Delta = \Delta_1 \Delta_2^2,$$

ist M das kleinste gemeinsame Multiplum von Ω_1, Δ_1, ferner $\theta_1, \theta_2, \ldots \theta_m$ diejenigen verschiedenen Primfaktoren von Θ, für welche

$$\left(\frac{-\Delta_\varkappa' \cdot f}{\theta_\varkappa}\right) = \left(\frac{-\Omega_\varkappa' \cdot \mathfrak{F}}{\theta_\varkappa}\right) = +1$$

ist, während

$$\left.\begin{aligned} \Delta_\varkappa' &= \frac{\Delta_1}{\theta_\varkappa} \text{ oder } = \Delta_1 \\ \Omega_\varkappa' &= \frac{\Omega_1}{\theta_\varkappa} \text{ oder } = \Omega_1 \end{aligned}\right\} \text{ ist, jenachdem } \theta_\varkappa \text{ in } \begin{cases} \Delta_1 \\ \Omega_1 \end{cases}$$

aufgeht oder nicht, ist endlich 2^n die Anzahl der verschiedenen unter den Werthsystemen

$$\left(\frac{d_1}{\theta_1}\right), \left(\frac{d_2}{\theta_2}\right), \ldots \left(\frac{d_m}{\theta_m}\right),$$

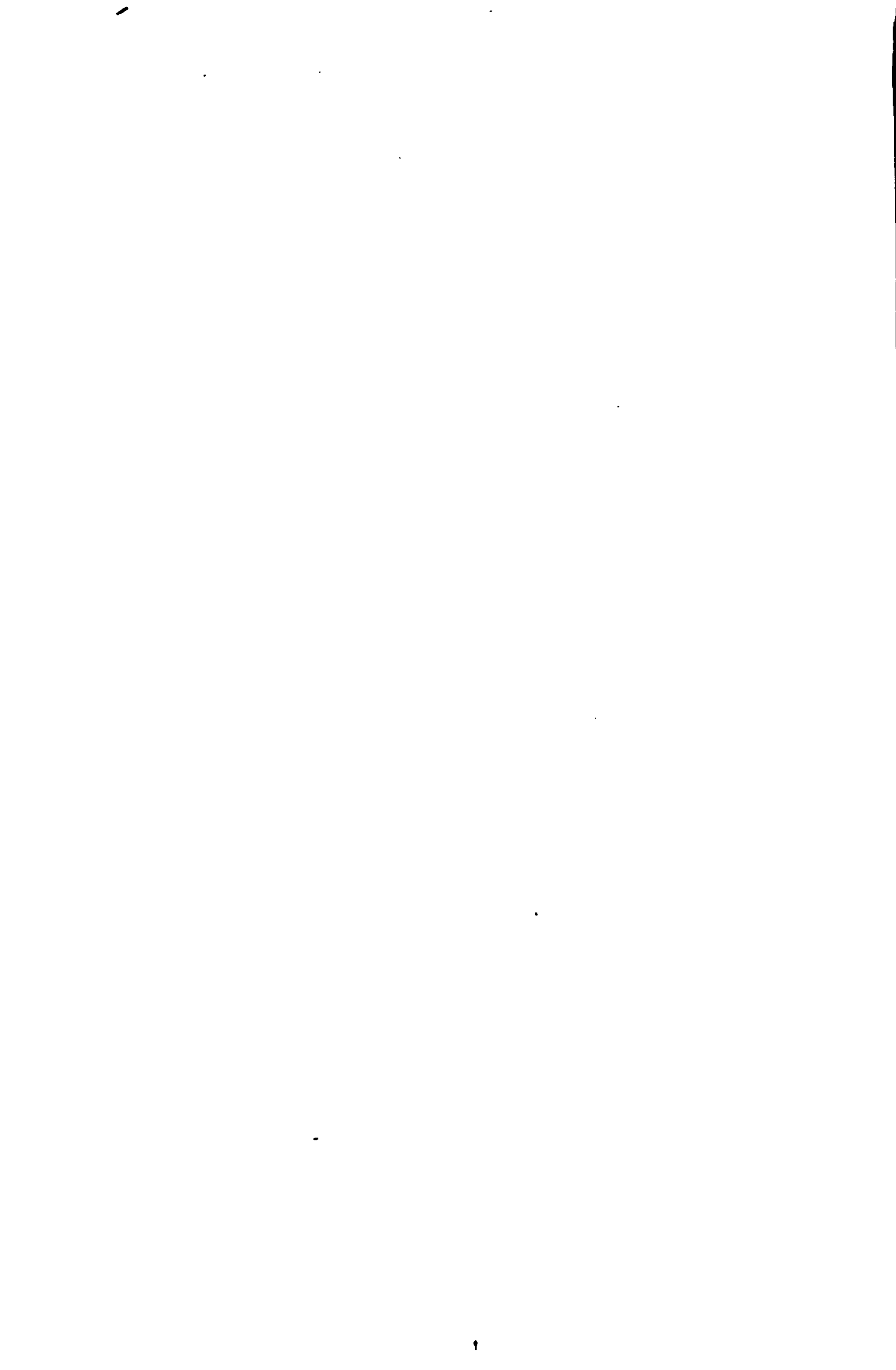
welche den sämmtlichen, positiven und negativen Theilern d von $2M$ entsprechen, wo wieder $d_\varkappa$ gleich $\frac{d}{\theta_\varkappa}$ oder d ist, jenachdem $\theta_\varkappa$ in d aufgeht oder nicht, so

ist die Classenanzahl des Geschlechts G, zu welchem die Form f mit der Reciproken $\mathfrak{F}$ gehört, gleich 2^{m-n}.

Besonders interessant erscheint in diesem Satze die wesentliche Bedeutung, welche die Primfaktoren $\theta_1, \theta_2, \ldots \theta_m$ für die Classenanzahl des Geschlechts besitzen, eine Bedeutung, welche Meyer veranlasst hat, diese Primfaktoren als Grundfaktoren des Geschlechts zu bezeichnen. —

Zum Schluss dieser Betrachtungen erwähnen wir schon hier einer Untersuchung von Eisenstein*), durch welche sich auch für bestimmte Formen die Classenanzahl ermitteln lässt; doch kann dieselbe und die interessanten Bemerkungen, zu welchen sie Anlass giebt, geeigneter Weise erst im dritten Abschnitte dieses Werkes ihre Darstellung finden.

*) S. Eisenstein's im siebenten Capitel erwähnte Arbeit, Monatsb. d. Berl. Ak. 1852.



ZWEITER ABSCHNITT.

DIE

ALLGEMEINEN QUADRATISCHEN FORMEN.

Wir haben unsere Betrachtungen bisher ausschliesslich auf *ternäre* quadratische Formen beschränkt und sowohl mit diesem Gange der Untersuchung als in der Art der Darstellung der geschichtlichen Entwickelung der Lehre Rechnung getragen, zugleich aber auch ein *Muster* hergestellt, nach welchem wir es nun unternehmen wollen, die *allgemeine* Theorie der quadratischen Formen d. i. diejenige der quadratischen Formen mit n Unbestimmten zu entwickeln. Bei der Verallgemeinerung der Untersuchungen traten aber den Forschern nicht nur manche Fragen oder Umstände, welche in dem einfacheren Falle der ternären Formen nicht zur Geltung kamen, überhaupt eine viel grössere Mannigfaltigkeit entgegen, sondern die Erkenntniss vertiefte sich auch, indem allgemeine Theorieen als Grundlage der Betrachtungen und mehr die obwaltenden *wesentlichen* Verhältnisse erkannt wurden. Es ist ein besonderes Verdienst namentlich der bezüglichen Arbeiten von *Minkowski*, die Theorie der quadratischen Formen ohne irgend beschränkende Voraussetzungen in *voller Allgemeinheit* behandelt zu haben. Mussten wir uns aber bereits bei den ternären Formen, um unserm ohnehin schon sehr umfangreichen Werke nicht zu weite Ausdehnung zu geben, auf Formen mit *ungerader Determinante* beschränken, so werden wir dazu bei der allgemeinen Theorie umsomehr genöthigt sein; wir werden es wenigstens thun, soweit es geschehen kann, ohne dass *wesentliche* Seiten des Gegenstandes unbeleuchtet bleiben oder die auftretenden Fragen und Sätze in charakteristischen Umständen eine Einbusse erleiden. Andererseits werden wir genöthigt sein, der Theorie der *quadratischen* Formen diejenige der *linearen* als ihre eigentliche Grundlage voraufzuschicken. Die letztere ist zuerst

hauptsächlich von Stephen Smith in einer schönen Abhandlung*), demnächst von Frobenius**) sehr eingehend bearbeitet worden. Man findet eine elegante Darstellung namentlich von des Ersteren Resultaten in einer Arbeit von Stieltjes***), doch wird sich die unsrige in ihren Grundlagen wie in dem Gange, den sie nimmt, wesentlich von der dortigen unterscheiden.

Erstes Capitel.

Algebraische Hilfssätze.

1. Wir müssen dabei die Lehre von den Determinanten in weiterem Umfange als bekannt voraussetzen, wollen jedoch zur Einleitung des Ganzen hier die hauptsächlichsten Sätze derselben, die wir anzuwenden haben, kurz zusammenstellen. Es sind zunächst folgende drei:

1) Sind in einer Determinante zwei Zeilen oder zwei Spalten identisch, so verschwindet sie.

2) Sind die Elemente einer Reihe

$$c_1 = a_1 + b_1, \quad c_2 = a_2 + b_2, \cdots c_n = a_n + b_n,$$

so ist die Determinante die Summe zweier anderen, in welchen jene Reihen resp. aus den Elementen:

$$a_1, a_2, \cdots a_n$$
$$b_1, b_2, \cdots b_n$$

bestehen, während die übrigen Reihen unverändert bleiben.

3) Der Multiplikationssatz, nach welchem

$$|a_{\alpha\beta}| \cdot |b_{\alpha\beta}| = |c_{\alpha\beta}|$$

ist, wenn man setzt:

$$c_{\alpha\beta} = a_{\alpha 1} b_{1\beta} + a_{\alpha 2} b_{2\beta} + \cdots + a_{\alpha n} \cdot b_{n\beta}.$$

---

*) On Systems of Linear Indeterminate Equations and Congruences, Philos. Transactions vol. 151 p. 293.

**) Theorie der linearen Formen mit ganzen Coefficienten, Journal für Mathematik, Bd. 86 und 88.

***) Sur la théorie des nombres Chap. III, in Annales de la faculté des sciences de Toulouse Bd. 4.

Sind ferner n Grössen $x_1, x_2, \dots x_n$ mit ebenso viel anderen Grössen $X_1, X_2, \dots X_n$ durch n Gleichungen

$$(1) \qquad X_\alpha = a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha n} x_n \quad (\alpha = 1, 2, \cdots n)$$

verbunden, deren Determinante oder Modulus

$$(2) \qquad A = | a_{\alpha\beta} |$$

von Null verschieden ist, so können die Gleichungen aufgelöst werden und ergeben, wenn zur Abkürzung

$$(3) \qquad A \cdot x_\alpha = \xi_\alpha$$

gesetzt wird, das adjungirte System linearer Gleichungen:

$$(4) \qquad \xi_\alpha = A_{1\alpha} X_1 + A_{2\alpha} X_2 + \cdots + A_{n\alpha} X_n, \quad (\alpha = 1, 2, \cdots n)$$

sowie nachstehende Beziehungen:

$$(5) \qquad \begin{cases} A = a_{\alpha 1} A_{\alpha 1} + a_{\alpha 2} A_{\alpha 2} + \cdots + a_{\alpha n} A_{\alpha n} & (\alpha = 1, 2, \cdots n) \\ 0 = a_{\alpha 1} A_{\beta 1} + a_{\alpha 2} A_{\beta 2} + \cdots + a_{\alpha n} A_{\beta n} & (\alpha \gtrless \beta) \end{cases}$$

sowie gleicherweise:

$$(5a) \qquad \begin{cases} A = a_{1\alpha} A_{1\alpha} + a_{2\alpha} A_{2\alpha} + \cdots + a_{n\alpha} A_{n\alpha} & (\alpha = 1, 2, \cdots n) \\ 0 = a_{1\alpha} A_{1\beta} + a_{2\alpha} A_{2\beta} + \cdots + a_{n\alpha} A_{n\beta} & (\alpha \gtrless \beta) \end{cases}$$

zwischen den Elementen $a_{\alpha\beta}$ der Determinante A und den ihnen resp. adjungirten Elementen $A_{\alpha\beta}$. Aus ihnen folgt nach dem Multiplikationssatze

$$(6) \qquad A \cdot \mathsf{A} = A^n$$

also

$$(7) \qquad \mathsf{A} = A^{n-1},$$

wenn A die Determinante der adjungirten Elemente d. i. die Determinante oder den Modulus der Gleichungen (4) bezeichnet. Ferner ist

$$(8) \qquad A_{\alpha\beta} = \frac{\partial A}{\partial a_{\alpha\beta}}$$

und, in Determinantenform ausgedrückt:

$$(9)\quad A_{\alpha\beta} = (-1)^{\alpha+\beta} \cdot \begin{vmatrix} a_{11} & \cdots a_{1,\beta-1} & a_{1,\beta+1} & \cdots a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{\alpha-1,1} & \cdots a_{\alpha-1,\beta-1} & a_{\alpha-1,\beta+1} & \cdots a_{\alpha-1,n} \\ a_{\alpha+1,1} & \cdots a_{\alpha+1,\beta-1} & a_{\alpha+1,\beta+1} & \cdots a_{\alpha+1,n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdots a_{n,\beta-1} & a_{n,\beta+1} & \cdots a_{nn} \end{vmatrix}$$

also, bis auf das Vorzeichen, diejenige Unterdeterminante erster Ordnung von A, welche nach Ausscheidung der Zeile α und der Spalte β übrig bleibt.

Wählen wir allgemeiner nach Belieben m Zeilen und ebensoviel Spalten aus, deren Indices resp.

$$\alpha\beta\gamma\cdots,\ \varrho\sigma\tau\cdots$$

seien, und der Grösse nach geordnet sein mögen. Die $m \cdot m$ Elemente der Determinante, in denen jene sich durchkreuzen, bilden eine Unterdeterminante m^{ten} Grades oder $n-m^{\text{ter}}$ Ordnung von A, welche wir durch das Symbol

$$(10)\qquad A^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots}$$

bezeichnen wollen. Sie findet sich in der entwickelten Determinante A in den adjungirten Faktor

$$(11)\qquad \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} = \frac{\partial^m A}{\partial a_{\alpha\varrho}\,\partial a_{\beta\sigma}\,\partial a_{\gamma\tau}\cdots}$$

multiplicirt, welcher bis auf das Vorzeichen diejenige Unterdeterminante von A ist, welche übrig bleibt, wenn jene m Zeilen und Spalten ausgeschieden werden; es ist nämlich

$$(12)\quad \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} = (-1)^{\alpha+\beta+\cdots+\varrho+\sigma+\cdots} \cdot A^{(n-m)}_{\alpha'\beta'\cdots,\varrho'\sigma'\cdots},$$

wenn $\alpha'\beta'\cdots,\varrho'\sigma'\cdots$ die dann übrig bleibenden Zeilen und Spalten bezeichnen. Es bestehen folgende Beziehungen, welche die Gleichungen (5) als einfachsten Fall ($m=1$) in sich enthalten:

$$(13)\quad \begin{cases} A = \sum\limits_{\varrho\sigma\tau\cdots} A^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} \cdot \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} \\ 0 = \sum\limits_{\varrho\sigma\tau\cdots} A^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} \cdot \overline{A}^{(m)}_{\alpha'\beta'\gamma'\cdots,\varrho\sigma\tau\cdots}; \end{cases}$$

in der zweiten dieser Formeln bedeutet $\alpha'\beta'\gamma'\cdots$ eine von

$\alpha\beta\gamma\cdots$ verschiedene, wie diese geordnete Combination, und in beiden Formeln erstreckt sich die Summation auf sämmtliche geordnete Combinationen $\varrho\sigma\tau\cdots$ von je m Elementen der Reihe $1, 2, 3, \cdots n$. Jede Determinante n^{ten} Grades ist hiernach eine homogene lineare Funktion derjenigen Unterdeterminanten vom Grade $m < n$, welche sich aus beliebigen m ihrer Zeilen (oder Spalten) bilden lassen.

Lässt man sowohl $\alpha\beta\gamma\cdots$ als $\varrho\sigma\tau\cdots$ sämmtliche geordnete Combinationen durchlaufen, so gewinnt man zwei Determinanten:

$$\left| A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \right| \quad \text{und} \quad \left| \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \right|$$

von μ^2 Elementen, wenn

$$\mu = \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdot 3\cdots m}$$

ist, und die Formeln (13) lehren sogleich mittels des Multiplikationssatzes die Gleichung

$$(14) \qquad \left| A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \right| \cdot \left| \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \right| = A^{\mu}.$$

Die Formel (6) ist hierin als der besondere Fall $m = n - 1$ enthalten. Aus der vorstehenden Formel ergiebt sich auch jeder der beiden Faktoren zur Linken als eine Potenz von A, insbesondere hat man

$$(14\text{a}) \qquad \left| A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \right| = A^{\lambda},$$

wo

$$\lambda = \frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}$$

ist*).

Bildet man aber auch für die Determinante A der adjungirten Elemente die Unterdeterminanten, so besteht zwischen ihnen und den Unterdeterminanten der ursprünglichen Determinante A die allgemeine Beziehung:

$$(15) \qquad \mathsf{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} = A^{m-1} \cdot \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots}.$$

Unter den Formeln, welche zwischen Unterdeterminanten verschiedener Ordnung stattfinden, haben wir von der folgenden:

---

*) S. Franke im J. f. Math. 61 S. 350—355.

(16) $$A \cdot \frac{\partial^2 A}{\partial a_{\alpha\beta} \partial a_{\gamma\delta}} = \frac{\partial A}{\partial a_{\alpha\beta}} \cdot \frac{\partial A}{\partial a_{\gamma\delta}} - \frac{\partial A}{\partial a_{\alpha\delta}} \cdot \frac{\partial A}{\partial a_{\gamma\beta}}$$

mehrfachen Gebrauch zu machen.

Endlich haben wir häufig eine Formel zu benutzen, nach welcher man für eine Determinante, die das Produkt zweier oder mehrerer Determinanten ist, die Unterdeterminanten einer gegebenen Ordnung aus den Unterdeterminanten derselben Ordnung der einzelnen Faktoren bilden kann. Ist

$$C = | a_{\alpha 1} b_{1\beta} + a_{\alpha 2} b_{2\beta} + \cdots + a_{\alpha n} b_{n\beta} |$$

die aus den Determinanten

$$A = \begin{vmatrix} a_{11} \, a_{12} \cdots a_{1n} \\ a_{21} \, a_{22} \cdots a_{2n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{n1} \, a_{n2} \cdots a_{nn} \end{vmatrix}, \quad B = \begin{vmatrix} b_{11} \, b_{12} \cdots b_{1n} \\ b_{21} \, b_{22} \cdots b_{2n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ b_{n1} \, b_{n2} \cdots b_{nn} \end{vmatrix}$$

zusammengesetzte Determinante von n^2 Elementen, so lautet diese Formel folgendermassen:

(17) $$C^{(m)}_{\alpha\beta\gamma\cdots,\,\alpha'\beta'\gamma'\cdots} = \sum_{\varrho\sigma\tau\cdots} A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \cdot B^{(m)}_{\varrho\sigma\tau\cdots,\,\alpha'\beta'\gamma'\cdots}$$

und die Summation darin erstreckt sich auf alle verschiedenen aus m Zahlen $\varrho\sigma\tau\cdots$ gebildeten (geordneten) Combinationen der Reihe $1, 2, 3, \cdots n$. Dieselbe lässt sich ohne weiteres auf eine aus mehr als zwei Faktoren zusammengesetzte Determinante ausdehnen. Der Formel zufolge ist also in der zusammengesetzten Determinante jede Unterdeterminante m^{ten} Grades eine homogene lineare Funktion von Unterdeterminanten desselben Grades von jeder einzelnen der Determinanten, aus denen jene zusammengesetzt ist.

2. Durch die Gleichungen (1) drückt man n Grössen X_1, $X_2, \cdots X_n$ durch n andere $x_1, x_2, \cdots x_n$ aus oder setzt diese an die Stelle der ersteren. Wir nennen deshalb diese Gleichungen eine Substitution und wollen dieselbe durch S_a bezeichnen. Die Determinante $| a_{\alpha\beta} |$ wird der Modulus der Substitution genannt. Wird letzterer von Null verschieden vorausgesetzt und kurz

(18) $$\frac{A_{i\varkappa}}{A} = \alpha_{i\varkappa}$$

geschrieben, so nehmen die Gleichungen (4) die Gestalt an:

$$x_i = \alpha_{1i} X_1 + \alpha_{2i} X_2 + \cdots + \alpha_{ni} X_n \tag{19}$$
$$(i = 1, 2, \cdots n)$$

und bilden die Auflösung der Gleichungen (1) oder die umgekehrte oder reciproke Substitution, welche durch S_a^{-1} bezeichnet werden soll. Man sieht: Wenn der Substitutionsmodulus von Null verschieden ist, entspricht vermittelst der Substitution jedem Werthsysteme x_1, $x_2 \cdots x_n$ ein einziges bestimmtes Werthsystem $X_1, X_2, \cdots X_n$ und umgekehrt.

Diese Betrachtung bedarf einer Einschränkung, falls es sich um ganzzahlige Werthsysteme handelt. Wird nämlich die Substitution (1), d. h. ihre Coefficienten als ganz vorausgesetzt, so ist zwar einleuchtend, dass jedem ganzzahligen Systeme $x_1, x_2, \cdots x_n$ nach (1) auch ein ganzzahliges System $X_1, X_2, \cdots X_n$ entspricht und, falls $A = \pm 1$ ist, auch umgekehrt; aber diese Bedingung $A = \pm 1$ ist auch erforderlich. In der That, wenn jedem ganzzahligen Systeme $X_1, X_2, \cdots X_n$ auch ein solches System $x_1, x_2, \cdots x_n$ nach (19) entsprechen soll, müssen sämmtliche $\alpha_{i\varkappa}$ ganze Zahlen sein, da z. B. $\alpha_{\varkappa 1}$, $\alpha_{\varkappa 2}, \cdots \alpha_{\varkappa n}$ dasjenige System $x_1, x_2, \cdots x_n$ ist, welches der Annahme, dass $X_\varkappa = 1$, die übrigen X gleich 0 sind, entspricht; alsdann aber folgt aus (18)

$$\frac{|A_{i\varkappa}|}{A^n} = |\alpha_{i\varkappa}|$$

als eine ganze Zahl und folglich wegen (7) $A = \pm 1$. Hieraus ergiebt sich der für alles Folgende fundamentale Satz: Damit bei einer ganzzahligen Substitution ganzzahligen Werthen der einen Reihe auch solche Werthe der anderen Reihe der Variabeln entsprechen, und umgekehrt, ist nothwendig und hinreichend, dass der Modulus der Substitution gleich ± 1 sei.

3. Werden in den Gleichungen (1) die Unbestimmten $x_1, x_2, \cdots x_n$ mittels einer neuen Substitution S_b:

$$x_\alpha = b_{\alpha 1} x_1' + b_{\alpha 2} x_2' + \cdots + b_{\alpha n} x_n' \tag{20}$$
$$(\alpha = 1, 2, \cdots n)$$

durch andere Unbestimmte $x_1', x_2', \cdots x_n'$ ersetzt, so nehmen

jene die Gestalt an:

$$(21) \qquad X_\alpha = c_{\alpha 1} x_1' + c_{\alpha 2} x_2' + \cdots + c_{\alpha n} x_n', \qquad (\alpha = 1, 2, \cdots n)$$

worin

$$(22) \qquad c_{\alpha\beta} = a_{\alpha 1} b_{1\beta} + a_{\alpha 2} b_{2\beta} + \cdots + a_{\alpha n} b_{n\beta} \qquad (\alpha, \beta = 1, 2, \cdots n)$$

gesetzt ist. Die Gleichungen (21) stellen auch eine Substitution S_c dar, bei welcher die Unbestimmten $X_1, X_2, \cdots X_n$ durch die dritte Reihe von Unbestimmten $x_1', x_2', \cdots x_n'$ ersetzt werden. Man nennt sie die aus den Substitutionen S_a, S_b zusammengesetzte Substitution und schreibt

$$(23) \qquad S_c = S_a \cdot S_b,$$

wo aber die Reihenfolge der Faktoren oder der Substitutionen zu beachten ist. — Auf solche Weise ist zugleich aus den zwei Systemen von je $n \cdot n$ Zahlen:

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ . & . & . & . \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{matrix} \quad \text{und} \quad \begin{matrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ . & . & . & . \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{matrix},$$

die wir kurz die Systeme $(a_{\alpha\beta})$, $(b_{\alpha\beta})$ oder a, b nennen wollen, gemäss der Formel (22) ein drittes System $(c_{\alpha\beta})$ oder c:

$$\begin{matrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ . & . & . & . \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{matrix}$$

entstanden, welches wir analog das aus a, b zusammengesetzte Zahlensystem

$$(24) \qquad c = a \cdot b$$

nennen wollen.

Fasst man, um mit Frobenius zu reden, diese Systeme „unter dem Bilde bilinearer Formen“ zusammen, indem man ihnen resp. die bilinearen Formen

$$(25) \qquad F_a = \Sigma a_{\alpha\beta} x_\alpha y_\beta, \quad F_b = \Sigma b_{\alpha\beta} x_\alpha y_\beta, \quad F_c = \Sigma c_{\alpha\beta} x_\alpha y_\beta$$

entsprechen lässt, so können wir die Zusammensetzung der Substitutionen oder der Systeme auch als Zusammensetzung bilinearer Formen deuten. Die aus F_a, F_b zusammenge-

setzte bilineare Form

$$F_c = F_a \cdot F_b \tag{26}$$

erweist sich dabei ohne Mühe als identisch mit der folgenden:

$$F_c = \sum_{\varkappa=1}^{n} \frac{\partial F_a}{\partial y_\varkappa} \cdot \frac{\partial F_b}{\partial x_\varkappa}. \tag{27}$$

Die Gesetze dieser Zusammensetzung werden für alle drei Fälle: die Substitutionen, die Zahlensysteme und die bilinearen Formen dieselben sein. Sie führen zu einer Rechnung mit solchen Elementen, welche in weiter Ausdehnung von Frobenius in seiner, im 84. Bd. des Journ. f. Math. enthaltenen Arbeit „über lineare Substitutionen und bilineare Formen" entwickelt worden ist. Wir dürfen uns hier damit begnügen, nur die fundamentalsten Sätze dieser Rechnung abzuleiten.

4. Unter $a \pm b$ verstehen wir dasjenige System von $n \cdot n$ Zahlen $a_{\alpha\beta} \pm b_{\alpha\beta}$, welches unter dem Bilde der bilinearen Form $F_a \pm F_b$ zusammengefasst erscheint. Ist hierdurch die Addition und Subtraktion für Zahlensysteme resp. bilineare Formen festgesetzt, so ergiebt sich die Definition der Multiplikation aus den gleichbedeutenden Formeln (24) oder (26). Dieser Multiplikation kommt im allgemeinen die Eigenschaft der Commutativität nicht zu, dagegen besitzt sie die beiden Eigenschaften der Distributivität und der Associativität, d. h. man hat die Gleichungen:

$$(a' + a'')b = a'b + a''b, \quad a(b' + b'') = ab' + ab''$$

also allgemeiner:

$$(a' + a'')(b' + b'') = a'b' + a'b'' + a''b' + a''b''$$

und die andere Gleichung:

$$(ab)c = a(bc). \tag{28}$$

Die ersteren folgen ohne weiteres aus der Formel (22); die Formel (28) bestätigt sich gleicherweise aus der Definition der Zusammensetzung von Systemen, am elegantesten durch den Nachweis der entsprechenden Gleichheit

$$(F_a F_b) F_c = F_a (F_b F_c), \tag{29}$$

den wir folgendermassen leisten. Nach (27) entsteht die Form $F_a F_b$, indem man entweder in

$$F_a = \sum_\varkappa \frac{\partial F_a}{\partial y_\varkappa} y_\varkappa$$

die Veränderlichen $y_\varkappa$ durch $\frac{\partial F_b}{\partial x_\varkappa}$ d. h. durch gewisse lineare Funktionen der $y_\varkappa$, oder in

$$F_b = \sum_\varkappa x_\varkappa \frac{\partial F_b}{\partial x_\varkappa}$$

die Veränderlichen $x_\varkappa$ durch $\frac{\partial F_a}{\partial y_\varkappa}$ d. h. durch gewisse lineare Funktionen der $x_\varkappa$ ersetzt. Hiernach wird man $(F_a F_b) F_c$ finden, indem man zuerst in F_b auf die Veränderlichen $x_\varkappa$ die Substitution $\frac{\partial F_a}{\partial y_\varkappa}$ und sodann auf die Veränderlichen $y_\varkappa$ die Substitution $\frac{\partial F_c}{\partial x_\varkappa}$ zur Anwendung bringt, während man durch umgekehrte Ausführung dieser Operationen aus F_b die Form $F_b F_c$ und dann $F_a(F_b F_c)$ hervorbringt. Da aber offenbar die Reihenfolge beider Operationen gleichgiltig ist, ergiebt sich die Gleichung (29).

Von selbst leuchtet noch die fernere Formel

$$(\gamma a) b = a(\gamma b) = \gamma(ab) \tag{30}$$

ein, in welcher γ eine Constante bedeutet.

Nach den aufgestellten Gesetzen kann man gegebene Systeme oder Formen in ganzer rationaler Weise d. h. durch die drei ersten Grundoperationen mit einander beliebig verknüpfen oder ganze Funktionen derselben herstellen.

Man nennt zwei Systeme a, b vertauschbar, wenn die Gleichheit besteht

$$a \cdot b = b \cdot a.$$

Ohne Schwierigkeit leuchtet dann ein: wenn jedes Glied einer Reihe $a, b, c, \cdots$ von Systemen (Formen) mit jedem Gliede einer anderen Reihe $a', b', c', \cdots$ einzeln vertauschbar ist, so ist's auch jede ganze Funktion von Gliedern der ersteren Reihe mit jeder ganzen Funktion von Gliedern der zweiten.

Das System a', welches aus a durch Vertauschung seiner Zeilen mit seinen Spalten entsteht:

$$\begin{matrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{matrix}$$

resp. die Form

$$F_a' = \Sigma a_{\beta\alpha} x_\alpha y_\beta,$$

welche aus F_a entsteht, wenn die Variabelnreihen mit einander vertauscht werden, soll nach Jacobi zu a resp. zu F_a conjugirt genannt werden. Offenbar ist die Conjugirte zu γa gleich $\gamma a'$, diejenige von $a + b$ ist $a' + b'$, und die Conjugirte von ab d. i. vom Systeme der Zahlen

$$a_{\alpha 1} b_{1\beta} + a_{\alpha 2} b_{2\beta} + \cdots + a_{\alpha n} b_{n\beta}$$

ist das System der Zahlen

$$b_{1\alpha} a_{\beta 1} + b_{2\alpha} a_{\beta 2} + \cdots + b_{n\alpha} a_{\beta n}$$

d. i. das aus den conjugirten Systemen b' und a' zusammengesetzte System $b'a'$.

Ist mithin ein System (eine Form) aus mehreren anderen zusammengesetzt, so ist es das conjugirte System (die conjugirte Form) aus den conjugirten der letzteren in umgekehrter Reihenfolge.

Die Gleichung

$$c = a \cdot b = 0 \tag{31}$$

ist gleichbedeutend mit dem Bestehen der $n \cdot n$ Gleichungen

$$c_{\alpha\beta} = a_{\alpha 1} b_{1\beta} + a_{\alpha 2} b_{2\beta} + \cdots + a_{\alpha n} b_{n\beta} = 0. \tag{32}$$
$$(\alpha = 1, 2, \cdots n;\ \beta = 1, 2, \cdots n)$$

Ist nun die Determinante A von Null verschieden, so erfordern diejenigen n dieser Gleichungen, welche

$$b_{1\beta}, b_{2\beta}, \cdots b_{n\beta}$$

enthalten, das gleichzeitige Verschwinden der letzteren Grössen; und da dies für jedes β gilt, so folgt aus (31) die Gleichung

$$b = 0$$

d. h. das Verschwinden aller Elemente des Systems b. Unter derselben Voraussetzung giebt es ein aber nur ein System x:

$$\begin{matrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ x_{1n} & x_{2n} & \cdots & x_{nn}, \end{matrix}$$

welches der Gleichung

$$(22) \qquad a \cdot x = b$$

Genüge leisten, wie aus den diese Beziehung aussprechenden Gleichungen

$$a_{r1}x_{1s} + a_{r2}x_{2s} + \cdots + a_{rn}x_{ns} = b_{rs}$$
$$r = 1, 2, \ldots n; \quad s = 1, 2, \ldots n$$

auf gleiche Weise hervorgeht*). Nun entsteht, wenn wieder A von Null verschieden ist, durch Zusammensetzung von a mit dem Systeme

$$\begin{matrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn}, \end{matrix}$$

welches durch a^{-1} bezeichnet werde, zufolge der Gleichungen (5) und (18) das einfache System

$$\begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 1, \end{matrix}$$

---

*) Hiernach giebt es auch ein einziges System y, für welches

$$y \cdot a = b$$

ist; denn dem Bewiesenen zufolge giebt es ein einziges System x, für welches

$$a' \cdot x = b'$$

ist, und hieraus folgt

$$x' \cdot a = b$$

also eine Lösung $y = x'$ der gestellten Gleichung. Eine zweite Lösung $y = z'$ kann es aber nicht geben, weil sonst

$$a' \cdot z = b'$$

also

$$a' \cdot (z - x) = 0$$

$$z = x$$

sich ergäbe.

das wir das System e nennen wollen, in Zeichen:

$$(34) \qquad a \cdot a^{-1} = e,$$

und zufolge der Gleichungen (5a) ebenso

$$(34a) \qquad a^{-1} \cdot a = e.$$

Das durch jede der Gleichungen (34), (34a) eindeutig definirte System a^{-1} soll das zu a reciproke System genannt werden; seine Determinante ist offenbar ebenfalls reciprok zur Determinante des ersteren. Es ist einleuchtend, dass jedes System ohne sich zu ändern mit dem System e in beliebiger Reihenfolge zusammengesetzt werden kann; letzteres spielt also bei der Zusammensetzung die Rolle der Einheit.

Hat auch das System b eine von Null verschiedene Determinante B, so gehört zu b ein reciprokes System b^{-1}. Aus den Gleichheiten

$$ab \cdot b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = a \cdot a^{-1} = e$$

folgt dann sogleich die Beziehung:

$$(ab)^{-1} = b^{-1} \cdot a^{-1}$$

oder der Satz: Ist ein System von nicht verschwindender Determinante aus mehreren anderen zusammengesetzt, so ist es das reciproke System aus den reciproken Systemen der letzteren in umgekehrter Reihenfolge.

Da $e' = e$ ist, folgt aus (34a) $a' \cdot (a^{-1})' = e$, und da gleichzeitig $a' \cdot (a')^{-1} = e$ ist, folgt

$$(a^{-1})' = (a')^{-1}$$

d. h. das zum reciproken Systeme conjugirte ist zugleich das reciproke des conjugirten Systems.

Ist a mit b vertauschbar und B nicht Null, so kann man

$$\begin{aligned} a \cdot b^{-1} &= (b^{-1}b) \cdot (ab^{-1}) = b^{-1}(ba)b^{-1} \\ &= b^{-1}(ab)b^{-1} = (b^{-1}a)(bb^{-1}) = b^{-1} \cdot a \end{aligned}$$

setzen, d. h. dann ist auch a mit b^{-1} vertauschbar. Bei diesen Voraussetzungen wollen wir schreiben:

$$(35) \qquad a \cdot b^{-1} = b^{-1} \cdot a = \frac{a}{b}$$

und auf solche Weise den Quotienten zweier Systeme

definiren. — Zugleich wird dann die Determinante von b' nicht Null, a', b' aber vertauschbar sein. Das conjugirte System zu $\frac{a}{b}$ ist alsdann $\frac{a'}{b'}$; denn wegen (35) ist es sowohl gleich

$$(b^{-1})' \cdot a' = (b')^{-1} \cdot a'$$

als auch gleich

$$a' \cdot (b^{-1})' = a' \cdot (b')^{-1}$$

also gleich $\frac{a'}{b'}$. — Ist A ebenfalls von Null verschieden, so existirt auch der Quotient $\frac{b}{a}$, und man findet, dass $\frac{b}{a}$ das zu $\frac{a}{b}$ reciproke System ist. In der That ist $\frac{b}{a} = a^{-1} \cdot b$, und das zu $\frac{a}{b} = b^{-1} \cdot a$ reciproke System ist das aus den Reciproken von b^{-1} und a, d. i. aus b und a^{-1} in umgekehrter Folge zusammengesetzte System also dem vorigen gleich.

Durch die letzten Betrachtungen sind wir in den Stand gesetzt, so oft wir nur vertauschbare Systeme betrachten, aus beliebig gegebenen Systemen auch gebrochene, allgemein also rationale Funktionen zu bilden. Und man überzeugt sich auf Grund der gegebenen Sätze ohne Schwierigkeit, dass, wenn zwei Systeme von nicht verschwindender Determinante mit einander vertauschbar sind, auch jede rationale Funktion des einen vertauschbar ist mit jeder rationalen Funktion des anderen. Insbesondere sind stets zwei rationale Funktionen desselben Systems von nicht verschwindender Determinante unter einander vertauschbar.

Zweites Capitel.

Von den Elementartheilern der Zahlensysteme.

1. Indem wir hiermit diese Betrachtungen vorläufig verlassen, wenden wir uns zur Theorie der linearen Formen.

Jeder Ausdruck

$$a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n,$$

in welchem $a_{11}, a_{12}, \cdots a_{1n}$ ganze Zahlen sind, heisst eine lineare Form mit n Unbestimmten $x_1, x_2, \cdots x_n$. Die sich hier darbietende Hauptfrage ist die: welche ganzen Zahlen kann die Form liefern oder darstellen, wenn den Unbestimmten alle möglichen ganzzahligen Werthe beigelegt werden? Diese Frage kommt im Grunde auf die Aufgabe hinaus: alle etwa vorhandenen ganzzahligen Auflösungen der unbestimmten Gleichung

$$(1) \qquad a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = a_1,$$

in welcher a_1 eine beliebig gegebene ganze Zahl ist, zu ermitteln. Die gestellte Frage kann aber als einfachster Fall der allgemeineren untergeordnet werden: Welche Systeme von m ganzen Zahlen $a_1, a_2 \cdots a_m$ können gleichzeitig durch m lineare Formen

$$(2) \qquad A_\alpha = a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n \qquad (\alpha = 1, 2, \cdots m)$$

mittels ganzer Werthe der Unbestimmten $x_1, x_2, \cdots x_n$ dargestellt werden, resp. welches sind die sämmtlichen ganzzahligen Auflösungen der m Gleichungen

$$(3) \qquad a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n = a_\alpha ? \qquad (\alpha = 1, 2, \cdots m)$$

Diesen m Gleichungen ist das ganzzahlige System a ihrer $m \cdot n$ Coefficienten

$$(4) \qquad \left\{ \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix} \right.$$

zugehörig, welches, wenn m von n verschieden ist, im Gegensatz zu den bisher betrachteten quadratischen Zahlensystemen vom Typus $n \cdot n$ als rechteckiges Zahlensystem vom Typus $m \cdot n$ bezeichnet werden soll. Indem man aus diesem Systeme nach Belieben $\varkappa$ Zeilen und $\varkappa$ Spalten auswählt, kann man aus ihm eine gewisse Anzahl Determinanten $\varkappa^{\text{ten}}$ Grades bilden, und so gehören zu ihm eine gewisse Anzahl Determinanten 1ten, 2ten, 3ten Grades u. s. w. bis zu Determinanten m^{ten} Grades, wenn $m < n$, oder Determinanten n^{ten} Grades, wenn $m > n$ ist.

Geschieht es hierbei, dass sämmtliche Determinanten $\varkappa^{\text{ten}}$ Grades gleich Null sind, so gilt dasselbe auch von allen Determinanten $\varkappa + 1^{\text{ten}}$ Grades, denn, indem man diejenigen $\varkappa + 1^{\text{ten}}$ Grades nach den Elementen einer Zeile entwickelt, werden sie lineare homogene Funktionen von Determinanten $\varkappa^{\text{ten}}$ Grades also Null. Wenn nun r so beschaffen ist, dass sämmtliche Determinanten $r + 1^{\text{ten}}$ Grades des Systems a verschwinden, nicht aber sämmtliche Determinanten r^{ten} Grades, so soll r der Rang des Systems a heissen. Dieser Rang ist höchstens gleich der kleineren der beiden Zahlen m, n.

Wir bezeichnen mit $d_\varkappa$ den (positiv genommenen) grössten gemeinsamen Theiler aller aus a hervorgehenden Determinanten $\varkappa^{\text{ten}}$ Grades, falls diese nicht sämmtlich verschwinden, entgegengesetzten Falles die Null. Demnach sind $d_1, d_2, \cdots d_r$ positive ganze Zahlen, $d_{r+1}, \cdots d_m$, wenn $m < n$, und $d_{r+1}, \cdots d_n$, wenn $m > n$ ist, gleich Null. Da, wie bemerkt, jede Determinante $\varkappa + 1^{\text{ten}}$ Grades eine lineare homogene Funktion von solchen $\varkappa^{\text{ten}}$ Grades ist, also durch den grössten gemeinsamen Theiler $d_\varkappa$ aller letzteren aufgeht, so ist auch $d_{\varkappa+1}$ theilbar durch $d_\varkappa$ und jede der Zahlen $d_1, d_2, \cdots d_r$ durch die vorhergehenden theilbar; mithin ist, wenn $e_\varkappa = \frac{d_\varkappa}{d_{\varkappa-1}}$ gesetzt wird, jede der Zahlen $e_1, e_2, \cdots e_r$ eine positive ganze Zahl; wir setzen ferner $e_{r+1}, \cdots e_m$ resp. $e_{r+1} \cdots e_n$ gleich Null. Diese Zahlen $e_\varkappa$ nennen wir die Elementartheiler des Zahlensystems a.

2. Zur näheren Untersuchung der Auflösbarkeit der Gleichungen (3) machen wir nun Gebrauch von folgenden beiden Bemerkungen.

Erstens können wir die Gleichungen durch m andere gleichbedeutende ersetzen, wenn wir mit Hilfe von $m \cdot m$ ganzen Zahlen $p_{\alpha\beta}$, deren Determinante $P = 1$ ist, an Stelle der linearen Formen A_α die folgenden einführen:

$$A'_\alpha = p_{\alpha 1} A_1 + p_{\alpha 2} A_2 + \cdots + p_{\alpha m} A_m \tag{5}$$
$$(\alpha = 1, 2, \cdots m).$$

Wird nämlich zugleich

$$a'_\alpha = p_{\alpha 1} a_1 + p_{\alpha 2} a_2 + \cdots + p_{\alpha m} a_m \tag{6}$$
$$(\alpha = 1, 2, \cdots m)$$

gesetzt, so sind offenbar die Gleichungen (3) völlig gleichbedeutend mit den folgenden:

$$A'_\alpha = a'_\alpha \qquad (7)$$
$$(\alpha = 1, 2, \cdots m)$$

aus denen auch rückwärts jene wieder hervorgehen. Beide Systeme von Gleichungen sind also zugleich auflösbar oder nicht auflösbar und haben im ersteren Falle die nämlichen Auflösungen. Ausführlich geschrieben nehmen die Gleichungen (7) die Gestalt an:

$$a'_{\alpha 1}x_1 + a'_{\alpha 2}x_2 + \cdots + a'_{\alpha n}x_n = a'_\alpha, \qquad (7a)$$
$$(\alpha = 1, 2, \cdots m)$$

wo

$$a'_{\alpha\beta} = p_{\alpha 1}a_{1\beta} + p_{\alpha 2}a_{2\beta} + \cdots + p_{\alpha m}a_{m\beta} \qquad (8)$$
$$(\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots n)$$

gesetzt ist. Man sieht, dass die Elemente $a'_{\alpha\beta}$ des rechteckigen Zahlensystems $a^{(1)}$ vom Typus $m \cdot n$ aus denjenigen des quadratischen Systems p vom Typus $m \cdot m$ und denjenigen des rechteckigen Systems a vom Typus $m \cdot n$ auf ganz dieselbe Weise entstehen, wie nach (22) vor. nr. die $c_{\alpha\beta}$ aus den Elementen der zwei quadratischen Systeme a, b gebildet wurden; es lässt sich daher das System $a^{(1)}$ wieder als aus p und a zusammengesetzt bezeichnen:

$$a^{(1)} = p \cdot a,$$

und folglich stets ein System vom Typus $m \cdot m$ mit einem solchen vom Typus $m \cdot n$ zu einem Systeme des letzteren Typus zusammensetzen.

Zweitens können wir statt der Unbestimmten $x_1, x_2, \cdots x_n$ ebenso viel andere $y_1, y_2, \cdots y_n$ durch die ganzzahlige Substitution

$$x_\alpha = q_{\alpha 1}y_1 + q_{\alpha 2}y_2 + \cdots + q_{\alpha n}y_n \qquad (9)$$
$$(\alpha = 1, 2, \cdots n)$$

mit dem Modulus $Q = 1$ einführen, wodurch die lineare Form

$$A'_\alpha = a'_{\alpha 1}x_1 + a'_{\alpha 2}x_2 + \cdots + a'_{\alpha n}x_n$$

die neue Gestalt einer in den y linearen Form

$$B_\alpha = b_{\alpha 1}y_1 + b_{\alpha 2}y_2 + \cdots + b_{\alpha n}y_n \qquad (10)$$

annimmt, wenn man setzt

(11) $$b_{\alpha\beta} = a'_{\alpha 1} q_{1\beta} + a'_{\alpha 2} q_{2\beta} + \cdots + a'_{\alpha n} q_{n\beta}.$$
$$(\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots n)$$

Die Gleichungen (7) oder (7a) erhalten so die Gestalt:

(12) $$B_\alpha = a'_\alpha$$
$$(\alpha = 1, 2, \cdots m)$$

und, weil vermöge der Substitution (9) $B_\alpha = A'_\alpha$ ist und jedem ganzzahligen Systeme der x ein solches der y entspricht und umgekehrt, so leuchtet ein, dass aus jeder ganzzahligen Auflösung der gegebenen Gleichungen (3) oder (7a) eine solche der Gleichung (12) hervorgeht und umgekehrt. Man darf also an Stelle der ersteren Gleichungen die letzteren setzen; in den beiden Umformungen aber, durch welche diese aus jenen entstehen, ist die Möglichkeit geboten, dass durch passende Wahl der Zahlensysteme p und q die neuen Gleichungen den gegebenen gegenüber einfacher werden.

Hierauf werden wir also unsere Bemühungen richten. Vorher bemerken wir nur noch, dass den Gleichungen (11) gemäss das System b der Zahlen $b_{\alpha\beta}$ vom Typus $m \cdot n$ als zusammengesetzt betrachtet werden kann aus dem Systeme $a^{(1)}$ vom gleichen Typus und dem quadratischen Systeme q vom Typus $n \cdot n$, in Zeichen:

$$b = a^{(1)} \cdot q.$$

Man darf daher auch schreiben

(13) $$b = p \cdot a \cdot q$$

und findet mithin, wenn man ein rechteckiges System vom Typus $m \cdot n$ links mit einem quadratischen vom Typus $m \cdot m$, rechts mit einem solchen vom Typus $n \cdot n$ zusammensetzt, wieder ein rechteckiges System vom Typus $m \cdot n$. Unschwer erkennt man, dass auch diese Zusammensetzung von Zahlensystemen associativ d. h. dass

$$p \cdot (aq) = (pa) \cdot q$$

ist. Desgleichen ist

$$p \cdot (p_1 a) = (pp_1) \cdot a,\ (aq) \cdot q_1 = a \cdot (qq_1),$$

wenn p, p_1 zwei Zahlensysteme vom Typus $m \cdot m$; q, q_1 zwei solche vom Typus $n \cdot n$ sind.

Da die Determinante der Systeme p und q der Einheit gleich sind, wollen wir sie Einheitssysteme nennen. Ihre reciproken Systeme p^{-1}, q^{-1} sind dann ((34) vor. Cap.) auch Systeme ganzer Zahlen und zwar Einheitssysteme von demselben Typus wie p resp. q. Aus der Formel (13) geht aber offenbar noch folgende hervor:

$$a = p^{-1} \cdot b \cdot q^{-1}. \tag{14}$$

Denken wir uns eine Determinante $\varkappa^{\text{ten}}$ Grades des Systems $a^{(1)} = p \cdot a$, etwa diejenige, welche aus den Zeilen $i_1, i_2, \cdots i_\varkappa$ und den Spalten $h_1, h_2, \cdots h_\varkappa$ gebildet ist:

$$\begin{vmatrix} p_{i_1 1} a_{1 h_1} + \cdots + p_{i_1 m} a_{m h_1}, & \cdots p_{i_1 1} a_{1 h_\varkappa} + \cdots + p_{i_1 m} a_{m h_\varkappa} \\ p_{i_\varkappa 1} a_{1 h_1} + \cdots + p_{i_\varkappa m} a_{m h_1}, & \cdots p_{i_\varkappa 1} a_{1 h_\varkappa} + \cdots + p_{i_\varkappa m} a_{m h_\varkappa} \end{vmatrix};$$

den einfachsten Determinantensätzen zufolge ist sie eine Summe von so viel Gliedern, als aus den m Indices $1, 2, \cdots m$ sich $\varkappa$ verschiedene auswählen lassen, und jedes dieser Glieder ist eine (aus den Spalten $h_1, h_2, \cdots h_\varkappa$ gebildete) Determinante $\varkappa^{\text{ten}}$ Grades aus a mal einer Determinante $\varkappa^{\text{ten}}$ Grades aus p, mithin ist jede Determinante $\varkappa^{\text{ten}}$ Grades aus $a^{(1)}$ eine homogene lineare Funktion von Determinanten $\varkappa^{\text{ten}}$ Grades aus a und also jedenfalls durch den grössten gemeinsamen Theiler $d_\varkappa$ aller der letzteren theilbar; daher wird auch der grösste gemeinsame Theiler aller jener Determinanten durch $d_\varkappa$ theilbar sein. Ist aber p ein Einheitssystem, so folgt, da

$$a = p^{-1} \cdot a^{(1)}$$

gesetzt werden kann, dasselbe auch umgekehrt, und daher ist für beide Systeme der grösste gemeinsame Theiler all' jener Determinanten ein- und dieselbe Zahl $d_\varkappa$. Aus ganz entsprechenden Gründen leuchtet dasselbe ein für die beiden Systeme $a^{(1)}$ und $b = a^{(1)} \cdot q$, wenn auch q ein Einheitssystem ist, und somit findet sich der Satz: So oft in der Beziehung

$$b = p \cdot a \cdot q$$

p und q Einheitssysteme sind, sind für die beiden Systeme a, b desselben Typus die grössten gemeinsamen Theiler aller Determinanten desselben Grades und also auch ihr Rang und ihre Elementartheiler die gleichen.

3. Wir heben gewisse besondere Einheitssysteme p, q vor den übrigen hervor.

Verstehen wir unter $U_{i,\varkappa}$ die Substitution, welche

$$x_i \text{ in } -x_i', \quad x_\varkappa \text{ in } -x_\varkappa'$$

verwandelt, unter $T_{i,\varkappa}$ diejenige, welche

$$x_i \text{ in } x_\varkappa', \quad x_\varkappa \text{ in } -x_i'$$

überführt, endlich unter $S_{i,\pm\varkappa}$ diejenige, bei welcher

$$x_i \text{ in } x_i' \pm x_\varkappa'$$

übergeht, während jedesmal die übrigen Unbestimmten unverändert bleiben, so kommt allen diesen drei Substitutionen offenbar der Modulus 1 zu, die ihnen entsprechenden Coefficientensysteme sind folglich Einheitssysteme. Dasselbe gilt, wenn h eine positive ganze Zahl ist, von der Substitution, welche

$$x_i \text{ in } x_i' \pm h x_\varkappa'$$

verwandelt, da sie ersichtlicherweise nichts anderes ist, als die $h$mal wiederholte Substitution $S_{i,\pm\varkappa}$. Diese Substitutionen resp. die ihnen entsprechenden Zahlensysteme mögen als elementare vor allen übrigen ausgezeichnet werden. Wenn man nun ein Zahlensystem a links mit den, resp. $U_{i,\varkappa}$, $T_{i,\varkappa}$, $S_{i,\pm\varkappa}^h$ entsprechenden Zahlensystemen vom Typus $m \cdot m$ zusammensetzt, so wird die Wirkung, welche dadurch auf das System a hervorgebracht wird, wie sogleich einleuchtet, darin bestehen, dass bei $U_{i,\varkappa}$ die Zeilen $i, \varkappa$ entgegengesetzt genommen, bei $T_{i,\varkappa}$ dieselben mit einander vertauscht werden, wobei zugleich eine von ihnen das Vorzeichen verändert, bei $S_{i,\pm\varkappa}^h$ aber zur i^{ten} Zeile die $\varkappa^{\text{te}}$ mit h multiplicirt addirt resp. subtrahirt wird. Geschieht dagegen die Zusammensetzung von a zur Rechten mit elementaren Einheitssystemen vom Typus $n \cdot n$, so werden dieselben Veränderungen an den gleichen Spalten des Systems a hervorgebracht. Mit Hilfe dieser einfachen Bemerkungen wollen wir nun nach Kronecker*) zeigen, wie allein durch eine Reihe von solchen elementaren Zusammensetzungen jedes ganzzahlige Zahlensystem

*) Kronecker, Reduktion der Systeme von n^2 ganzzahligen Elementen, Journ. f. Math. 107 S. 135.

a auf eine einfache (reducirte) Form zurückgeführt werden kann.

Sind, was wir dabei stets voraussetzen können, nicht sämmtliche Zahlen des Systems a gleich Null, so giebt es unter ihnen eine oder mehrere von kleinstem Werthe. Durch eine Vertauschung von höchstens zwei Zeilen und zwei Spalten d. i. durch Zusammensetzung des Systems links oder rechts mit einem elementaren Systeme der zweiten Art, lässt sich eine dieser Zahlen an die erste Stelle des Systems bringen und eventuell darauf durch Zusammensetzung mit einem Systeme der ersten Art positiv machen. Sind dann nicht alle Elemente der ersten Zeile durch dies erste Element theilbar, z. B. nicht das $\varkappa^{\text{te}}$, so kann man, indem man ein passendes Vielfache der ersten Spalte von der $\varkappa^{\text{ten}}$ subtrahirt, d. i. durch Zusammensetzung zur Rechten mit einem passenden Systeme der dritten Art das $\varkappa^{\text{te}}$ Element positiv und kleiner machen als das erste, worauf es sich wieder an die erste Stelle bringen lässt u. s. w., bis nothwendig nach einer beschränkten Anzahl solcher Operationen alle Elemente der ersten Zeile durch das dann an erster Stelle stehende positive Element theilbar sein werden. Offenbar können sie dann durch mehrfache Zusammensetzung zur Rechten mit Systemen der dritten Art sämmtlich ausser dem ersten, das unverändert bleibt, zu Null gemacht werden. — Sollte nunmehr noch nicht jedes Element der ersten Spalte, z. B. nicht das $\varkappa^{\text{te}}$, durch das erste theilbar sein, so könnte man es, indem man die erste Zeile mit einer passenden ganzen Zahl multiplicirt von der $\varkappa^{\text{ten}}$ subtrahirt, d. i. durch Verwendung eines geeigneten Zahlensystems der dritten Art auf der linken Seite positiv und kleiner machen als das erste, und darauf mit dem so bereits erhaltenen Systeme den ganzen Process von Neuem beginnen. Da jedesmal dabei das an erster Stelle stehende Element verkleinert wird, muss nothwendigerweise nach einer endlichen Anzahl solcher Processe die erste Zeile ausser dem ersten Gliede lauter Nullen, die erste Spalte aber lauter durch das erste Glied theilbare Elemente enthalten, und alsdann können diese letzteren durch Verwendung einer Reihe von Systemen der dritten Art auf der linken Seite ebenfalls auf Null gebracht werden.

Gesetzt nun, in dem so reducirten Systeme a käme noch ein Element vor, welches nicht durch das erste theilbar ist, so addire man durch Zusammensetzung mit einem Systeme der dritten Art zur Linken die entsprechende Zeile zur ersten, wodurch das Anfangsglied ungeändert bleibt, und mache dann, indem man die erste Spalte, mit einer passenden Zahl multiplicirt, zur Spalte jenes Elementes addirt, d. i. durch Zusammensetzung mit einem geeigneten Systeme der dritten Art auf der rechten Seite das fragliche Element positiv und kleiner als das erste. Sogleich lässt sich der ganze Process von Neuem beginnen, wobei stets das Anfangsglied sich verringert; nach einer endlichen Anzahl von Wiederholungen muss man daher endlich das System a auf ein anderes reduciren, bei welchem die erste Zeile und Spalte ausser dem positiven Anfangsglied nur Nullen enthalten, jedes andere Glied aber durch das Anfangsglied theilbar ist. Das reducirte System hat also die Gestalt:

$$\begin{matrix} \eta_1 & 0 & \cdots & 0 \\ 0 & \mathfrak{a}_{22} & \cdots & \mathfrak{a}_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \mathfrak{a}_{m2} & \cdots & \mathfrak{a}_{mn} \end{matrix} ,$$

wo $\eta_1 > 0$ und jedes $\mathfrak{a}_{\alpha\beta}$ durch η_1 theilbar ist.

Jetzt aber lässt sich offenbar, ohne dass die erste Zeile und Spalte verändert wird, das Zahlensystem der $\mathfrak{a}_{\alpha\beta}$, wenn es nicht aus lauter Nullen besteht, auf genau dieselbe Weise weiter reduciren, wobei die Theilbarkeit seiner Elemente durch η_1 augenscheinlich durch die auszuführenden Operationen nicht aufgehoben werden kann, u. s. f., und so wird folglich zuletzt ein System von folgender Gestalt:

$$m\left\{\begin{matrix} \overbrace{\begin{matrix} \eta_1 & 0 & \cdots & & 0 & \cdot \\ 0 & \eta_2 & \cdots & & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \eta_\varrho & 0 & \cdot \\ 0 & 0 & \cdots & 0 & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{matrix}}^{n} \end{matrix}\right.$$

hervorgehen, in welchem $\eta_1, \eta_2, \cdots \eta_\varrho$ positive ganze Zahlen sind, von denen jede in der folgenden als Theiler enthalten ist*). Ein solches System, in welchem alle Glieder ausserhalb der „Diagonale"**) Null sind, möge hinfort ein Diagonalsystem genannt werden. Bezeichnen wir das in Rede stehende mit E und bedenken, dass die Zusammensetzung der Systeme associativ ist, und dass die sämmtlichen bei der Reduktion sei es links, sei es rechts zur Zusammensetzung verwandten Systeme Einheitssysteme waren, also unter sich zusammengesetzt wieder gewisse Einheitssysteme p und q liefern, so können wir das erreichte Resultat einfach in folgendem Fundamentalsatz zusammenfassen:

Das System a vom Typus $m \cdot n$ kann durch Zusammensetzung mit einem Einheitssysteme p vom Typus $m \cdot m$ zur Linken, und einem solchen Systeme q vom Typus $n \cdot n$ zur Rechten in ein Diagonalsystem E verwandelt werden, sodass die Gleichung besteht:

$$(15) \qquad p \cdot a \cdot q = E.$$

Hier ist aber ein Zusatz von grosser Wichtigkeit. Man bemerkt leicht, dass im Systeme E alle Determinanten, deren Grad $> \varrho$ ist, verschwinden, nicht aber sämmtliche Determinanten vom Grade ϱ. Da a vom Range r ist, folgt demnach aus dem Satze am Schlusse vor. nr., dass $\varrho = r$ sein muss. Dann ist aber jede Determinante aus E, deren Grad $\varkappa \overline{\gtrless} r$ ist, wenn sie nicht verschwindet, durch $\varkappa$ der Zahlen $\eta_1, \eta_2, \cdots \eta_r$ und, da jede von diesen durch die vorhergehende, mithin jedes Produkt aus $\varkappa$ von ihnen durch das Produkt der $\varkappa$ ersten aufgehen muss, durch $\eta_1 \cdot \eta_2 \cdots \eta_\varkappa$ theilbar, während die aus den ersten $\varkappa$ Zeilen und Spalten gebildete Determinante diesem Produkte gleich ist; das Produkt $\eta_1 \cdot \eta_2 \cdots \eta_\varkappa$ ist

---

*) Möglicherweise, wenn nämlich $\varrho = m < n$ oder $\varrho = n < m$ ist, fallen die letzten, nur aus Nullen bestehenden Zeilen resp. Spalten weg; und wenn $\varrho = m = n$ ist, wird η_ϱ nicht stets positiv sein, sondern dasselbe Vorzeichen haben müssen, wie die Determinante A.

**) Wir behalten diesen leicht verständlichen Ausdruck, der eigentlich nur bei quadratischen Systemen zutreffend ist, der Kürze wegen auch bei rechteckigen Systemen bei.

folglich grösster gemeinsamer Theiler aller Determinanten $\varkappa^{\text{ten}}$ Grades von E, also dem angezogenen Satze zufolge

$$d_\varkappa = \eta_1 \eta_2 \cdots \eta_\varkappa$$

ebenso

$$d_{\varkappa-1} = \eta_1 \eta_2 \cdots \eta_{\varkappa-1}$$

also $\frac{d_\varkappa}{d_{\varkappa-1}} = e_\varkappa$ gleich $\eta_\varkappa$ Man findet folglich:

Das Diagonalsystem E, welches in der Formel (15) auftritt, muss die Form haben:

$$\begin{matrix} e_1 & 0 & \cdots & & 0 & \cdot \\ 0 & e_2 & \cdots & & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & e_r & 0 & \cdot \\ 0 & 0 & \cdots & 0 & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{matrix},$$

wo die nur Nullen enthaltenden Zeilen resp. Spalten ausfallen, so oft der Rang r gleich m resp. n ist; die reducirte Form des Zahlensystems a ist also eine eindeutig bestimmte. Da $e_\varkappa = \eta_\varkappa$ gefunden worden, so ist der Herleitung gemäss jede der Zahlen $e_1, e_2, \cdots e_r$ in der folgenden enthalten, also der Quotient $\frac{e_\varkappa}{e_{\varkappa-1}}$ eine ganze Zahl.

4. Wenn a, b ganzzahlige Systeme desselben Typus $m \cdot n$ sind, zwischen welchen die Beziehung

$$b = p \cdot a \cdot q \tag{16}$$

besteht, während p, q ganzzahlige Einheitssysteme resp. vom Typus $m \cdot m$ und $n \cdot n$ sind, so ist auch umgekehrt

$$a = p^{-1} \cdot b \cdot q^{-1},$$

wo p^{-1}, q^{-1} gleichfalls solche Systeme sind. In diesem Falle nennen wir die Systeme a, b einander äquivalent. Zur Aequivalenz zweier Systeme a, b (desselben Typus) ist nothwendig und hinreichend, dass sie gleichen Rang und gleiche Elementartheiler haben. Dass dies nothwendig sei, ist bereits in dem Schlusssatze von nr. 2 ausgesprochen; dass es auch hinreicht, ergiebt sich aus dem Fundamentalsatze (15), wie folgt: haben a, b gleichen Rang und

gleiche Elementartheiler, so kann man

$$p \cdot a \cdot q = E, \quad r \cdot b \cdot s = E$$

machen, wo p, r und q, s Einheitssysteme je des gleichen Typus sind; hieraus folgt aber

$$r \cdot b \cdot s = p \cdot a \cdot q$$

also

$$b = r^{-1}p \cdot a \cdot qs^{-1},$$

wo nun $r^{-1}p$, qs^{-1}, weil aus Einheitssystemen resp. von gleichem Typus zusammengesetzt, wieder solche sind.

Besteht allgemeiner zwischen a, b die Beziehung (16), während p, q beliebige quadratische Systeme vom Typus $m \cdot m$ und $n \cdot n$ resp. sind, so wollen wir, eine Gauss'sche Ausdrucksweise verallgemeinernd, b unter a enthalten nennen. Die Aequivalenz ist somit nur ein besonderer Fall des Enthaltenseins. Alsdann lässt sich folgender Satz beweisen:

Damit ein System b unter einem Systeme a (desselben Typus) enthalten sei, ist nothwendig und hinreichend, dass der Rang des Systems b nicht grösser ist als der von a, und dass die Elementartheiler von b Vielfache der entprechenden Elementartheiler von a sind*).

Um diesen Satz zu begründen, betrachten wir zuvörderst zwei quadratische Systeme a, b vom Typus $n \cdot n$ und das aus ihnen zusammengesetzte quadratische System c desselben Typus. Sind $a_{\alpha\beta}$, $b_{\alpha\beta}$, $c_{\alpha\beta}$ die Elemente dieser drei Systeme, so besteht die allgemeine Beziehung:

$$c_{\alpha\beta} = a_{\alpha 1}b_{1\beta} + a_{\alpha 2}b_{2\beta} + \cdots + a_{\alpha n}b_{n\beta}.$$

Ist nun r der Rang von a, so kann man zwei Einheitssysteme p, q vom Typus $n \cdot n$ angeben, so beschaffen, dass das zusammengesetzte System $p \cdot a \cdot q$ das folgende wird:

*) Dieser Satz ist (in einer andern Einkleidung) zuerst von Frobenius in seiner grossen Abhandlung „Theorie der linearen Formen mit ganzen Coefficienten“ im Journ. f. Math. 86 und 88, und zwar in letzterem Bande S. 114 bewiesen worden. Einen andern, dem hier dargestellten näherstehenden Beweis gab Hensel „über die Elementartheiler componirter Systeme“ in dems. Journal 114 S. 109.

$$E = \begin{array}{ccccccc} e_1 & 0 & \cdots & 0 & 0 & \cdot \\ 0 & e_2 & \cdots & 0 & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & e_r & 0 & \cdot \\ 0 & 0 & \cdots & & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array},$$

wo $e_1, e_2, \cdots e_r$ die r von Null verschiedenen Elementartheiler von a sind, und man kann setzen:

$$d = p \cdot c = (paq) \cdot (q^{-1}b) = E \cdot g,$$

wo g ein quadratisches System von $n \cdot n$ Zahlen ist, welche $g_{\alpha\beta}$ heissen mögen; diese Gleichheit lehrt offenbar, dass das Zahlensystem d mit dem folgenden:

$$\begin{array}{cccc} e_1 g_{11} & e_1 g_{12} & \cdots & e_1 g_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ e_r g_{r1} & e_r g_{r2} & \cdots & e_r g_{rn} \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

vom Typus $n \cdot n$ übereinstimmt. Nun ist aber erstlich, da d aus der Zusammensetzung eines Einheitssystems mit c hervorgeht, der grösste gemeinsame Theiler $d_\varkappa'$ aller Unterdeterminanten $\varkappa^{\text{ten}}$ Grades von d gleich demjenigen von c. Man sieht, dass diese sämmtlich verschwinden, wenn $\varkappa > r$, dass also dann $d_\varkappa' = 0$ ist; für $\varkappa < r$ dagegen wird jede von Null verschiedene Unterdeterminante $\varkappa^{\text{ten}}$ Grades $D_\varkappa$ gleich dem Produkte aus $\varkappa$ von den Elementartheilern $e_1, e_2, \cdots e_r$ und der entsprechenden Unterdeterminante $G_\varkappa$ des Systems

$$\begin{array}{cccc} g_{11} & g_{12} & \cdots & g_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ g_{r1} & g_{r2} & \cdots & g_{rn} \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

sein, sodass wir setzen dürfen

$$D_\varkappa = e_{i_1} e_{i_2} \cdots e_{i_{\varkappa-1}} e_{i_\varkappa} \cdot G_\varkappa,$$

wenn $i_1 < i_2 < \cdots < i_\varkappa$ gewisse, der Grösse nach geordnete Indices der Reihe $1, 2, \cdots r$ bedeuten. Betrachten wir ferner diejenigen Unterdeterminanten $\varkappa - 1^{\text{ten}}$ Grades $D_{\varkappa-1}$, welche in der Determinante $D_\varkappa$ zu den Elementen ihrer letzten Zeile adjungirt sind, so dürfen wir analog

$$D_{\varkappa-1} = e_{i_1} e_{i_2} \cdots e_{i_{\varkappa-1}} \cdot G_{\varkappa-1}$$

setzen, und jede dieser Unterdeterminanten wird theilbar sein durch $d'_{\varkappa-1}$. Da aber $G_\varkappa$ eine homogene lineare Funktion der gedachten $G_{\varkappa-1}$ ist, so wird jedenfalls $D_\varkappa$ gleich $e_{i_\varkappa}$ mal einer homogenen linearen Funktion der gedachten $D_{\varkappa-1}$ und folglich durch $e_{i_\varkappa} \cdot d'_{\varkappa-1}$, umsomehr also durch

$$e_\varkappa \cdot d'_{\varkappa-1} = \frac{d_\varkappa}{d_{\varkappa-1}} \cdot d'_{\varkappa-1}$$

theilbar sein. Dies gilt daher auch vom grössten gemeinsamen Theiler $d_\varkappa'$ der sämmtlichen $D_\varkappa$, mögen sie Null oder von Null verschieden sein, und somit ist $d_\varkappa'$ theilbar durch

$$\frac{d_\varkappa}{d_{\varkappa-1}} \cdot d'_{\varkappa-1}$$

oder

$$\frac{d_\varkappa'}{d'_{\varkappa-1}} = e_\varkappa' \text{ theilbar durch } \frac{d_\varkappa}{d_{\varkappa-1}} = e_\varkappa.$$

Man erhält also zunächst folgenden Satz: Ist ein quadratisches System aus zwei (oder mehreren) solchen Systemen zusammengesetzt, so ist jeder seiner (von Null verschiedenen) Elementartheiler ein Vielfaches des entsprechenden Elementartheilers eines jeden einzelnen der Systeme*).

Zwar scheint der Satz durch das Vorhergehende nur bezüglich des ersten Faktors a bewiesen zu sein. Jedoch sind offenbar die Determinanten $\varkappa^{\text{ten}}$ Grades, welche aus einem Systeme a sich bilden lassen, denjenigen gleich, die aus dem conjugirten Systeme a' hervorgehen, somit auch die Zahlen

*) Der hier mitgetheilte Beweis des Satzes findet sich bei Frobenius „über die Elementartheiler der Determinanten" in den Sitzungsberichten der Berl. Ak. v. J. 1894, wo auch noch ein zweiter aus der Formel (19) dieses Capitels geschöpfter Beweis gegeben wird.

$d_\varkappa$ und die Reihe der Elementartheiler für beide dieselben. Ist aber $c = a \cdot b$, so ist $c' = b' \cdot a'$, dem Bewiesenen zufolge also die Elementartheiler von c' d. h. von c Vielfache der entsprechenden Elementartheiler von b' d. i. von b. —

5. Nunmehr betrachten wir ein **rechteckiges** System a vom Typus $m \cdot n$:

$$\begin{array}{llll} a_{11} & a_{12} & \cdots & a_{1n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \cdots & a_{mn}, \end{array}$$

wir setzen $m < n$ voraus; entgegengesetzten Falls gelten ähnliche Schlüsse. **Erweitert** man dies System durch Hinzufügung von $n - m$ Zeilen mit Nullen zu einem quadratischen Systeme a_0 vom Typus $n \cdot n$:

$$\begin{array}{llll} a_{11} & a_{12} & \cdots & a_{1n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ 0 & 0 & \cdots & 0 \\ . & . & . & ., \end{array}$$

so leuchtet ein, dass die Gesammtheit aller aus a gebildeten Determinanten vom Grade $\varkappa \overline{\overline{<}} m$ mit der Gesammtheit aller solchen aus a_0 gebildeten bis auf gewisse hinzutretende Determinanten des letzteren, welche Null sind, übereinstimmt, und somit wird die mit $d_\varkappa$ bezeichnete Zahl und folglich auch $e_\varkappa$ für beide Systeme, so lange $\varkappa \overline{\overline{<}} m$ ist, ein- und dieselbe sein. Ist ferner $a^{(1)}$ das aus dem quadratischen Systeme p:

$$\begin{array}{llll} p_{11} & p_{12} & \cdots & p_{1m} \\ . & . & . & . \\ p_{m1} & p_{m2} & \cdots & p_{mm} \end{array}$$

und a zusammengesetzte System

$$\begin{array}{llll} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ . & . & . & . \\ a'_{m1} & a'_{m2} & \cdots & a'_{mn}, \end{array}$$

so kann man das **erweiterte** System $a_0^{(1)}$:

$$\begin{matrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a'_{m1} & a'_{m2} & \cdots & a'_{mn} \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \end{matrix},$$

dessen Elementartheiler $e'_\varkappa$, wie bemerkt, so lange $\varkappa \overline{\gtrless} m$ ist, mit denjenigen von $a^{(1)}$ übereinstimmen, als zusammengesetzt ansehen aus dem quadratischen Systeme p_0:

$$\begin{matrix} p_{11} & p_{12} & \cdots & p_{1m} & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{m1} & p_{m2} & \cdots & p_{mm} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{matrix}$$

vom Typus $n \cdot n$ mit dem quadratischen Systeme a_0 vom gleichen Typus. Dem vorigen Satze zufolge werden mithin die (von Null verschiedenen) Elementartheiler von $a^{(1)}$ Vielfache der entsprechenden Elementartheiler von a sein.

Wenn nun das System $a^{(1)}$ vom Typus $m \cdot n$ mit dem quadratischen Systeme q vom Typus $n \cdot n$:

$$\begin{matrix} q_{11} & q_{12} & \cdots & q_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ q_{n1} & q_{n2} & \cdots & q_{nn} \end{matrix}$$

sich zu dem Systeme b:

$$\begin{matrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{matrix}$$

zusammensetzt, so entsteht offenbar aus dem erweiterten Systeme $a_0^{(1)}$ durch jene Zusammensetzung das erweiterte System b_0:

$$\begin{matrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mn} \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \end{matrix}$$

vom Typus $n \cdot n$ und seine (von Null verschiedenen) Elementartheiler, welche, so lange $\varkappa \overline{\overline{<}} m$ ist, mit denjenigen von b übereinstimmen, sind dem Hilfssatze zufolge Vielfache von den entsprechenden Elementartheilern von $a^{(1)}$, folglich auch von denjenigen von a. Soll also b unter a enthalten sein, so ist nothwendig, dass der Rang von b nicht grösser als der von a, und dass die Elementartheiler von b Vielfache der entsprechenden Elementartheiler von a sind.

Nehmen wir aber diese Bedingungen als erfüllt an, und bestimmen Einheitssysteme p, r und q, s resp. vom Typus $m \cdot m$ und $n \cdot n$, so dass

$$p \cdot a \cdot q = E, \quad r \cdot b \cdot s = E^{(1)}$$

wird, wo

$$E = \begin{matrix} e_1 & 0 & \cdots & 0 & \cdots \\ 0 & e_2 & \cdots & 0 & \cdots \\ . & . & . & . & . \\ 0 & 0 & \cdots & e_r & \cdots \\ 0 & 0 & \cdots & 0 & \cdots \\ . & . & . & . & . \end{matrix}, \quad E^{(1)} = \begin{matrix} e_1' & 0 & \cdots & 0 & \cdots \\ 0 & e_2' & \cdots & 0 & \cdots \\ . & . & . & . & . \\ 0 & 0 & \cdots & e_r' & \cdots \\ 0 & 0 & \cdots & 0 & \cdots \\ . & . & . & . & . \end{matrix}$$

und allgemein $e_\varkappa' = \eta_\varkappa \cdot e_\varkappa$ ist, während einige der letzten $\eta_\varkappa$ auch Null sein können. Offenbar wird auch

$$p_0 \cdot a_0 \cdot q = E_0, \quad r_0 \cdot b_0 \cdot s = E_0^{(1)}$$

sein, wenn wir durch den Index 0 die resp. nach dem Obigen zu Quadraten erweiterten Systeme bezeichnen, und man findet sogleich $E_0^{(1)}$ als zusammengesetzt aus dem Diagonalsysteme H_0:

$$\begin{matrix} \eta_1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ . & . & . & . & . & . & . & . \\ 0 & 0 & \cdots & \eta_r & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 1 & \cdots & \cdot \\ . & . & . & . & . & . & . & . \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{matrix}$$

vom Typus $n \cdot n$ und aus E_0. Hieraus folgt aber

$$b_0 = (r_0^{-1} H_0 p_0) \cdot a_0 \cdot (q s^{-1}).$$

Da nun, wie man sich leicht überzeugt, sowohl r_0^{-1} als auch

das zusammengesetzte System $r_0^{-1} H_0 p_0$ dieselbe Gestalt hat, wie das System p_0, so erschliesst man aus vorstehender Gleichung diese andere

$$b = \varpi \cdot a \cdot \varkappa,$$

wenn unter ϖ, $\varkappa$ gewisse quadratische Systeme vom Typus $m \cdot m$ resp. $n \cdot n$ verstanden werden, d. h. b ist unter a enthalten. Die obgenannten Bedingungen genügen also auch dazu, dass b unter a enthalten ist, und somit ist der zu Beweis gestellte Satz jetzt vollkommen erwiesen.

6. Zur Abkürzung der Ausdrucksweise führen wir an dieser Stelle zwei Benennungen ein. Ist $D_\varkappa$ irgend eine aus einem System a gebildete Determinante $\varkappa^{\text{ten}}$ Grades, so soll jede Unterdeterminante erster Ordnung von $D_\varkappa$, die also stets eine aus a gebildete Determinante $\varkappa - 1^{\text{ten}}$ Grades ist, kurz eine Subdeterminante von $D_\varkappa$ genannt werden; dagegen nennen wir jede aus a gebildete Determinante $\varkappa + 1^{\text{ten}}$ Grades, welche $D_\varkappa$ als Unterdeterminante erster Ordnung enthält, eine Superdeterminante von $D_\varkappa$ *).

Wenn man nun aus einem Systeme a:

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix}$$

irgend eine Determinante $\varkappa^{\text{ten}}$ Grades herausnimmt, so lässt sich ihr System stets als eine Zusammensetzung des Systems a mit quadratischen Systemen auffassen. In der That erkennt man z. B. das System

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1\varkappa} \\ \cdot & \cdot & \cdot & \cdot \\ a_{\varkappa 1} & a_{\varkappa 2} & \cdots & a_{\varkappa\varkappa} \end{matrix}$$

sogleich als Resultat der Zusammensetzung folgender drei Systeme:

*) Vgl. Hensel, über reguläre Determinanten und die aus ihnen abgeleiteten Systeme, Journ. f. Math. 114 S. 25.

$$\begin{matrix} 1\,0\cdots0\,0\cdots \\ 0\,1\cdots0\,0\cdots \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ 0\,0\cdots1\,0\cdots \\ 0\,0\cdots0\,0\cdots \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \end{matrix} \qquad \begin{matrix} a_{11}\;a_{12}\cdots a_{1n} \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ a_{m1}\;a_{m2}\cdots a_{mn} \end{matrix} \qquad \begin{matrix} 1\,0\cdots0\,0\cdots \\ 0\,1\cdots0\,0\cdots \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ 0\,0\cdots1\,0\cdots \\ 0\,0\;\cdot\;\cdot\;\cdot\;\cdot \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \end{matrix},$$

dessen erstes vom Typus $m \cdot m$, dessen letztes vom Typus $n \cdot n$ gedacht ist, während in beiden alle Glieder bis auf die ersten $\varkappa$ Diagonalglieder vom Werthe 1 gleich Null sind. Dem vorigen Satze zufolge darf man daher sagen: Ist $D_\varkappa$ irgend eine Determinante $\varkappa^{\text{ten}}$ Grades des Systems a, und $t_\varkappa$ der grösste gemeinsame Theiler aller ihrer Subdeterminanten, mithin $\frac{D_\varkappa}{t_\varkappa}$ ihr $\varkappa^{\text{ter}}$ Elementartheiler $\varepsilon_\varkappa$, so ist $\varepsilon_\varkappa$ ein Vielfaches von $e_\varkappa$. Denkt man sich diesen Quotienten für sämmtliche Determinanten $\varkappa^{\text{ten}}$ Grades von a gebildet, so wird folglich auch der grösste gemeinsame Theiler $\varDelta_\varkappa$ aller dieser Quotienten durch $e_\varkappa$ theilbar sein. Andererseits ist jedes $D_\varkappa$ theilbar durch $d_\varkappa$ und umsomehr $\frac{D_\varkappa}{d_{\varkappa-1}}$ eine ganze Zahl, und $t_\varkappa$, als grösster gemeinsamer Theiler gewisser Determinanten $\varkappa - 1^{\text{ten}}$ Grades von a, ist gewiss durch den grössten gemeinsamen Theiler dieser sämmtlichen Determinanten, d. i. durch $d_{\varkappa-1}$ theilbar. Demnach ist der Quotient

$$\frac{D_\varkappa}{d_{\varkappa-1}} : \frac{D_\varkappa}{t_\varkappa} = \frac{t_\varkappa}{d_{\varkappa-1}}$$

eine ganze Zahl oder $\frac{D_\varkappa}{d_{\varkappa-1}}$ durch $\frac{D_\varkappa}{t_\varkappa}$ und folglich auch durch $\varDelta_\varkappa$ theilbar. Da dies für jede der Determinanten $D_\varkappa$ gilt, muss auch der grösste gemeinsame Theiler aller Quotienten $\frac{D_\varkappa}{d_{\varkappa-1}}$ d. h. $\frac{d_\varkappa}{d_{\varkappa-1}} = e_\varkappa$ theilbar sein durch $\varDelta_\varkappa$. Aus beiden Resultaten erschliesst man die Gleichheit

$$\varDelta_\varkappa = e_\varkappa.$$

Hatten wir also bisher den Elementartheiler $e_\varkappa$ nur als Quotienten zweier grössten gemeinsamen Theiler definirt:

$e_\varkappa = \frac{d_\varkappa}{d_{\varkappa-1}}$, so zeigt sich jetzt $e_\varkappa$ selbst als ein grösster gemeinsamer Theiler bestimmt, wie folgt: Der $\varkappa^{\text{te}}$ Elementartheiler eines Systems ist der grösste gemeinsame Theiler der Quotienten, welche man erhält, wenn man jede Determinante $\varkappa^{\text{ten}}$ Grades des Systems durch den grössten gemeinsamen Theiler ihrer Subdeterminanten dividirt*).

Ist das System $\mathfrak{a}$ ein Theil eines Systems a, so wird jede Determinante $\varkappa^{\text{ten}}$ Grades aus $\mathfrak{a}$ auch eine solche von a und jeder Quotient aus einer Determinante $\varkappa^{\text{ten}}$ Grades von $\mathfrak{a}$ und dem grössten gemeinsamen Theiler ihrer Subdeterminanten auch einer der analogen Quotienten von a sein; mithin ist gewiss der $\varkappa^{\text{te}}$ Elementartheiler von $\mathfrak{a}$ als grösster gemeinsamer Divisor sämmtlicher jener Quotienten theilbar durch den grössten gemeinsamen Divisor dieser Quotienten d. i. durch den $\varkappa^{\text{ten}}$ Elementartheiler von a. Enthält also ein System a ein anderes $\mathfrak{a}$ als Theil, so geht der $\varkappa^{\text{te}}$ Elementartheiler des ersteren im $\varkappa^{\text{ten}}$ Elementartheiler des letzteren auf.

Ist ferner eine Primzahl p in den mit $d_\varkappa$, $d_{\varkappa-1}$, $D_\varkappa$, $t_\varkappa$ bezeichneten Zahlen genau resp. $\partial_\varkappa$, $\partial_{\varkappa-1}$, $\partial_\varkappa + \lambda$, $\partial_{\varkappa-1} + \lambda'$ Mal als Faktor enthalten, so sind λ, λ' nicht-negative Zahlen, und p ist in $e_\varkappa$ und $\frac{D_\varkappa}{t_\varkappa}$ genau $\partial_\varkappa - \partial_{\varkappa-1}$ resp. $\partial_\varkappa - \partial_{\varkappa-1} + \lambda - \lambda'$ Mal enthalten. Da $\frac{D_\varkappa}{t_\varkappa}$ durch $\Delta_\varkappa = e_\varkappa$ theilbar ist, findet sich $\lambda - \lambda' \geqq 0$. So oft also $\lambda = 0$ ist, muss auch $\lambda' = 0$ sein. Hieraus folgt der Satz: Ist $D_\varkappa$ eine Determinante $\varkappa^{\text{ten}}$ Grades, welche die Primzahl p genau so oft als Faktor enthält, als sie im grössten gemeinsamen Theiler $d_\varkappa$ aller solcher Determinanten aufgeht, so muss auch unter ihren Subdeterminanten eine sein, welche die Primzahl p in der gleichen Potenz enthält, wie $d_{\varkappa-1}$.

7. Bevor wir die grosse Reihe der Folgerungen weiter

---

*) Diese Definition fand zuerst Stephen Smith in seiner Abhandlung: On Systems of Linear Indeterminate Equations and Congruences, Phil. Trans. 151 p. 293.

entwickeln, welche die in der Formel (15) ausgesprochene Reduktion ganzzahliger Systeme zu ziehen gestattet, stellen wir ihr eine zweite ähnliche an die Seite.

Gesetzt wieder, r sei der Rang des Systems a, und zuerst $m < n$, so können wir durch eine eventuelle vorgängige Umformung, zu der es nur der Vertauschung gewisser Zeilen bedarf, bewirken, dass die aus den ersten r Zeilen möglichen Determinanten r^{ten} Grades nicht sämmtlich verschwinden; alsdann verschwinden auch, wenn $\varkappa < r$, nicht sämmtliche aus den ersten $\varkappa$ Zeilen möglichen Determinanten $\varkappa^{\text{ten}}$ Grades, denn jene können als lineare homogene Funktionen von diesen dargestellt werden. Ist dies geschehen, so sei allgemein $\tau_\varkappa$ grösster gemeinsamer Theiler aller Determinanten $\varkappa^{\text{ten}}$ Grades, die aus den ersten $\varkappa$ Zeilen herstellbar sind, sodass, da jede solche eine homogene lineare Funktion von Determinanten $\varkappa - 1^{\text{ten}}$ Grades ist, die aus den ersten $\varkappa - 1$ Zeilen herstellbar sind, jedenfalls $\frac{\tau_\varkappa}{\tau_{\varkappa-1}} = u_\varkappa$ eine ganze Zahl sein wird. Wenn man nun zur Rechten mit Einheitssystemen zusammensetzt, so erkennt man zuvörderst ganz wie bei der früheren Reduktion, dass die Zahlen $\tau_\varkappa$ also auch $u_\varkappa$ dabei ungeändert bleiben; denn die Determinanten $\varkappa^{\text{ten}}$ Grades, welche aus den ersten $\varkappa$ Zeilen gebildet werden, sind bei dem zusammengesetzten Systeme homogene lineare Funktionen derjenigen, welche bei dem ursprünglichen Systeme aus den ersten $\varkappa$ Zeilen gebildet sind, und umgekehrt; ferner sieht man, dass man diese Einheitssysteme so wählen d. h. die Spalten so mit einander verbinden kann, dass die erste Zeile die Gestalt annimmt:

$$\tau_1 = u_1, \; 0, \; 0, \; \cdots \; 0.$$

Ist dann

$$b_{21}, b_{22}, b_{23}, \cdots b_{2n}$$

die neue zweite Zeile, so können, wenn $r > 2$, nicht sämmtliche Zahlen $b_{22}, b_{23}, \cdots b_{2n}$ Null sein, da sonst sämmtliche aus den ersten zwei Zeilen genommenen Determinanten 2ten Grades Null wären, was, wie bemerkt, nicht sein kann. Daher haben dann $b_{22}, b_{23}, \cdots b_{2n}$ den grössten gemeinsamen Theiler u_2, und durch geeignete Verbindung der letzten $n-1$

Spalten kann man die zweite Zeile umformen in

$$b_{21},\ u_2,\ 0 \cdots 0,$$

und wenn man nun die zweite Spalte, mit einer passenden ganzen Zahl multiplicirt, zur ersten fügt, wodurch die erste Zeile ungeändert bleibt, b_{21} positiv und kleiner machen als u_2. Auf ähnliche Weise führt man sodann die dritte Zeile in die Gestalt

$$c_{31},\ c_{32},\ u_3,\ 0 \cdots 0$$

über, worin c_{31}, c_{32} positiv und kleiner sind als u_3 u. s. w. bis zur r^{ten} Zeile, welche die Form erhalten wird:

$$d_{r1},\ d_{r2},\ \cdots\ d_{r,r-1},\ u_r,\ 0 \cdots 0,$$

wo

$$d_{r1},\ d_{r2},\ \cdots\ d_{r,r-1}$$

positiv und kleiner sind als u_r. Sind nun überhaupt noch Zeilen vorhanden, so muss jede von ihnen die Gestalt haben:

$$\varkappa_1,\ \varkappa_2,\ \cdots\ \varkappa_{r-1},\ \varkappa_r,\ 0 \cdots 0,$$

damit jede Determinante $r+1^{\text{ten}}$ Grades Null sei. Man gelangt also durch Zusammensetzung mit Einheitssystemen zu einem System der folgenden Gestalt:

$$(17\text{a})\qquad \begin{cases} u_1 & 0 & 0 & \cdots & & 0 \cdots \\ b_{21} & u_2 & 0 & \cdots & & 0 \cdot\ \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\ \cdot \\ d_{r1} & d_{r2} & d_{r3} & \cdots & u_r & 0 \cdots \\ \varkappa_1 & \varkappa_2 & \varkappa_3 & \cdots & \varkappa_r & 0 \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\ \cdot \end{cases},$$

in welchem die letzten $n-r$ Spalten aus Nullen bestehen, die Zeilen von der $r+1^{\text{ten}}$ an aber ausfallen, wenn

$$r = m.$$

Wäre zweitens $m > n$, so würde nach einer eventuellen vorläufigen Vertauschung gewisser Spalten eine ähnliche Operation an den Zeilen d. h. eine Zusammensetzung mit Einheitssystemen auf der linken Seite das System a in die entsprechende Form

$$(17\text{b})\qquad \begin{cases} u_1 & b_{12} & \cdots & d_{1r} & h_1 & \cdots \\ 0 & u_2 & \cdots & d_{2r} & h_2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & d_{r-1,r} & h_{r-1} & \cdots \\ 0 & 0 & \cdots & u_r & h_r & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{cases}$$

überführen, in welcher die letzten $m - r$ Zeilen aus Nullen bestehen, die Spalten von der $r + 1^{\text{ten}}$ an aber ausfallen, wenn $r = n$.

8. Wir benutzen diese Resultate vor allem zum Beweise eines wichtigen Satzes*). Sei $D_{\varkappa-1}$ eine aus den Zeilen i_1, $i_2, \cdots i_{\varkappa-1}$ und den Spalten $h_1, h_2, \cdots h_{\varkappa-1}$, ebenso $D_\varkappa$ eine aus den Zeilen $f_1, f_2, \cdots f_\varkappa$ und den Spalten $g_1, g_2, \cdots g_\varkappa$ von a gebildete Determinante $\varkappa - 1^{\text{ten}}$ resp. $\varkappa^{\text{ten}}$ Grades, wobei es zulässig ist, dass die f sich theilweise mit den i, die g mit den h decken. Wir betrachten das Zahlensystem $\mathfrak{a}$:

$$\begin{matrix} a_{i_1 h_1} & \cdots & a_{i_1 h_{\varkappa-1}} & a_{i_1 g_1} & \cdots & a_{i_1 g_\varkappa} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{i_{\varkappa-1} h_1} & \cdots & a_{i_{\varkappa-1} h_{\varkappa-1}} & a_{i_{\varkappa-1} g_1} & \cdots & a_{i_{\varkappa-1} g_\varkappa} \\ a_{f_1 h_1} & \cdots & a_{f_1 h_{\varkappa-1}} & a_{f_1 g_1} & \cdots & a_{f_1 g_\varkappa} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{f_\varkappa h_1} & \cdots & a_{f_\varkappa h_{\varkappa-1}} & a_{f_\varkappa g_1} & \cdots & a_{f_\varkappa g_\varkappa}, \end{matrix}$$

welches aus $(2\varkappa - 1) \cdot (2\varkappa - 1)$ Elementen besteht und zur Abkürzung durch

$$\begin{matrix} a_{ih} & a_{ig} \\ a_{fh} & a_{fg} \end{matrix}$$

bezeichnet werden mag. Der zu beweisende Satz lautet dann so:

Das Produkt $D_{\varkappa-1} \cdot D_\varkappa$ ist theilbar durch das Produkt aus dem grössten gemeinsamen Theiler aller Subdeterminanten von $D_\varkappa$ und dem grössten gemeinsamen Theiler aller aus $\mathfrak{a}$ gebildeten Superdetermi-

*) Vgl. Frobenius in der zuletzt angeführten Arbeit.

nanten von $D_{\varkappa-1}$. Da nämlich das Rechteck der Elemente a_{fk} vom Typus $\varkappa(\varkappa-1)$ ist, kann das System $\mathfrak{a}$, indem man die letzte Reduktionsmethode zur Reduktion jenes Rechtecks verwendet, durch Zusammensetzung mit Einheitssystemen, die nur eine Vertauschung der ersten $\varkappa-1$ Spalten von $\mathfrak{a}$ bewirken und nur die letzten $\varkappa$ Zeilen verändern, in ein anderes $\mathfrak{a}'$ verwandelt werden, in welchem die letzte Zeile des genannten Rechtecks aus Nullen besteht; es sei folgendes:

$$\begin{matrix} a'_{ik} & a_{ig} \\ a'_{fk} & a'_{fg}, \end{matrix}$$

wobei dem Gesagten zufolge die Determinante $|a'_{ik}|$ numerisch gleich $|a_{ik}|$ d. i. gleich $D_{\varkappa-1}$ sein muss. Da zugleich das System a'_{fg} aus a_{fg} durch Zusammensetzung mit den angewandten Einheitssystemen der zuletzt genannten Art hervorgeht, muss sowohl die Determinante $|a'_{fg}|$ numerisch gleich $|a_{fg}|$ d. i. $D_\varkappa$, als auch der grösste gemeinsame Theiler $\mathfrak{D}_{\varkappa-1}$ aller Subdeterminanten für beide Determinanten derselbe sein. Endlich muss aber auch der grösste gemeinsame Theiler $\mathfrak{D}^{(\varkappa)}$ aller aus $\mathfrak{a}$ gebildeten Superdeterminanten von $|a_{ik}|$ demjenigen aller aus $\mathfrak{a}'$ gebildeten Superdeterminanten von $|a'_{ik}|$ gleich sein; denn, da jede der letzten $\varkappa$ Zeilen von $\mathfrak{a}'$ nur eine homogene lineare Verbindung der letzten $\varkappa$ Zeilen von $\mathfrak{a}$ sein kann, so ist jede von den letzteren Superdeterminanten auch eine homogene lineare Verbindung der ersteren, also jede von jenen durch den grössten gemeinsamen Theiler von diesen theilbar, und, weil nur Einheitssysteme zur Zusammensetzung benutzt wurden, auch umgekehrt. Betrachtet man aber insbesondere diejenigen Superdeterminanten von $|a'_{ik}|$, welche Elemente der letzten Zeile des Systems $\mathfrak{a}'$ enthalten, so sind diese gleich je einem Elemente der letzten Zeile von a'_{fg} mal $|a'_{ik}| = \pm D_{\varkappa-1}$, und folglich ist $d \cdot D_{\varkappa-1}$ ihr grösster gemeinsamer Theiler, wenn man mit d denjenigen aller Elemente der letzten Zeile von a'_{fg} bezeichnet; mithin ist jedenfalls $d \cdot D_{\varkappa-1}$ ein Vielfaches der Zahl $\mathfrak{D}^{(\varkappa)}$, die ein, allen aus $\mathfrak{a}'$ gebildeten Superdeterminanten von $|a'_{ik}|$ gemeinsamer Faktor ist.

Andererseits ist die Determinante $|a'_{fg}| = \pm D_\varkappa$, weil sie homogen und linear ist sowohl nach den Elementen ihrer

letzten Zeile als auch nach den Subdeterminanten ihrer $\varkappa - 1$ ersten Zeilen, theilbar durch $d \cdot \mathfrak{D}_{\varkappa-1}$. Daraus folgt, dass $dD_{\varkappa-1} \cdot D_\varkappa$ durch $\mathfrak{D}^{(\varkappa)} \cdot d\mathfrak{D}_{\varkappa-1}$ und folglich $D_{\varkappa-1}D_\varkappa$ durch $\mathfrak{D}^{(\varkappa)}\mathfrak{D}_{\varkappa-1}$ theilbar ist, w. z. b. w.

9. Ist nun p irgend eine Primzahl, so wollen wir mit $p^{\partial_\varkappa}$ die höchste Potenz derselben bezeichnen, welche in der Zahl $d_\varkappa$ aufgeht, wo $\partial_\varkappa = 0$ zu setzen ist, wenn $d_\varkappa$ diese Primzahl überhaupt nicht als Faktor enthält. Da

$$\frac{e_\varkappa}{e_{\varkappa-1}} = \frac{d_\varkappa}{d_{\varkappa-1}} : \frac{d_{\varkappa-1}}{d_{\varkappa-2}} = \frac{d_\varkappa d_{\varkappa-2}}{d_{\varkappa-1}^2}$$

eine ganze Zahl ist, ergiebt sich mit Bezug auf jede Primzahl p die Beziehung:

$$(18) \quad \partial_\varkappa + \partial_{\varkappa-2} - 2\partial_{\varkappa-1} \geqq 0 \text{ oder } \partial_\varkappa - \partial_{\varkappa-1} \geqq \partial_{\varkappa-1} - \partial_{\varkappa-2}.$$

Seien ferner $p^{\delta_\varkappa}$, $p^{\sigma_{\varkappa-1}}$ die höchsten Potenzen von p, welche in $D_\varkappa$ resp. in allen ihren Subdeterminanten und folglich in $\mathfrak{D}_{\varkappa-1}$, dagegen $p^{\delta_{\varkappa-1}}$, $p^{\sigma^{(\varkappa)}}$ diejenigen, welche in $D_{\varkappa-1}$ resp. in allen ihren aus a gebildeten Superdeterminanten und folglich in $\mathfrak{D}^{(\varkappa)}$ aufgehen: dann besteht dem letztbewiesenen Satze zufolge die zweite Ungleichheit:

$$(19) \qquad \delta_\varkappa + \delta_{\varkappa-1} \geqq \sigma^{(\varkappa)} + \sigma_{\varkappa-1}.$$

Wir entwickeln einige Folgerungen aus diesen beiden Ungleichheiten, führen aber zunächst mit Hensel zu diesem Zwecke eine bequeme Benennung ein. Weil nämlich $p^{\partial_\varkappa}$ die höchste in $d_\varkappa$ d. i. in sämmtlichen Unterdeterminanten $\varkappa^{\text{ten}}$ Grades des Systems a aufgehende Potenz von p ist, muss es unter den letzteren sicher eine geben, welche genau durch $p^{\partial_\varkappa}$ theilbar ist; jede solche Unterdeterminante wollen wir eine mit Bezug auf p reguläre Unterdeterminante $\varkappa^{\text{ten}}$ Grades nennen.

Nehmen wir nun erstens an, $D_\varkappa$ und $D_{\varkappa-1}$ seien regulär mit Bezug auf p. Dann ist

$$\delta_\varkappa = \partial_\varkappa, \quad \delta_{\varkappa-1} = \partial_{\varkappa-1}$$

und die Ungleichheit (19) nimmt die Form an:

$$\partial_\varkappa + \partial_{\varkappa-1} \geqq \sigma^{(\varkappa)} + \sigma_{\varkappa-1}.$$

Andererseits ist jede Superdeterminante von $D_{\varkappa-1}$ als Unter-

determinante $\varkappa^{\text{ten}}$ Grades (wenn sie nicht Null ist) durch $p^{\partial_\varkappa}$, und jede Subdeterminante von $D_\varkappa$ als Unterdeterminante $\varkappa - 1^{\text{ten}}$ Grades durch $p^{\partial_{\varkappa-1}}$ theilbar, also

$$\sigma^{(\varkappa)} \geqq \partial_\varkappa, \quad \sigma_{\varkappa-1} \geqq \partial_{\varkappa-1}$$

also

$$\sigma^{(\varkappa)} + \sigma_{\varkappa-1} \geqq \partial_\varkappa + \partial_{\varkappa-1},$$

was in Verbindung mit der obigen Ungleichheit sofort die Gleichheiten

$$\sigma^{(\varkappa)} = \partial_\varkappa, \quad \sigma_{\varkappa-1} = \partial_{\varkappa-1}$$

ergiebt. Demnach giebt es unter den aus $\mathfrak{a}$, umsomehr also unter den aus a gebildeten Superdeterminanten von $D_{\varkappa-1}$ mindestens eine, welche genau durch $p^{\partial_\varkappa}$, unter den Subdeterminanten von $D_\varkappa$ eine, welche genau durch $p^{\partial_{\varkappa-1}}$ theilbar ist, oder man erhält folgende zwei Sätze:

I. Jede mit Bezug auf p reguläre Determinante $\varkappa^{\text{ten}}$ Grades eines Systems a ($\varkappa > 1$) enthält eine solche reguläre Determinante $\varkappa - 1^{\text{ten}}$ Grades als Unterdeterminante.

II. Jede mit Bezug auf p reguläre Determinante $\varkappa - 1^{\text{ten}}$ Grades ($\varkappa$ nicht grösser als die kleinste der beiden Zahlen m, n) ist in einer solchen regulären Determinante $\varkappa^{\text{ten}}$ Grades als Unterdeterminante enthalten*).

Den ersten dieser beiden Sätze fanden wir bereits auf anderem Wege in nr. 6.

Wir wollen ferner eine Unterdeterminante $\varkappa^{\text{ten}}$ Grades — ohne Bezug auf eine bestimmte Primzahl — regulär nennen, wenn sie dem grössten Theiler $d_\varkappa$ aller solcher Unterdeterminanten numerisch gleich ist. Das System ihrer Subdeterminanten resp. das ihrer Superdeterminanten heisse regulär, wenn ihr grösster gemeinsamer Theiler gleich $d_{\varkappa-1}$ resp. gleich $d_{\varkappa+1}$

*) S. Hensel, über reguläre Determinanten etc. S. 29. Frobenius hat dieselben Sätze bewiesen im Sitzungsbericht d. B. Ak. 1894 S. 31—44; er erhält dort die Ungleichheit (19) aus einer von Kronecker (Journ. f. Math. 72 S. 158) gegebenen Determinanten-Identität.

ist. Aus den beiden erhaltenen Sätzen folgt dann der nachstehende*):

Ist eine Unterdeterminante $\varkappa^{\text{ten}}$ Grades regulär, so ist auch das System aller ihrer Subdeterminanten, wie auch dasjenige aller ihrer Superdeterminanten regulär. In der That ist die Determinante dann auch regulär in Bezug auf jede Primzahl p, unter ihren Subdeterminanten ist also eine, welche genau durch $p^{\partial_{\varkappa-1}}$ aufgeht, der grösste gemeinsame Theiler derselben enthält folglich jede Primzahl p genau ebenso oft wie $d_{\varkappa-1}$ und muss folglich gleich $d_{\varkappa-1}$ sein. In derselben Weise zeigt sich, dass der grösste gemeinsame Theiler aller Superdeterminanten der regulären Determinante $\varkappa^{\text{ten}}$ Grades gleich $d_{\varkappa+1}$ ist.

Eine weitere Folgerung aus den beiden obigen Sätze ist dieser andere:

Sind D_i und D_h zwei mit Bezug auf p reguläre Determinanten eines Systems resp. vom Grade i und h, ist D_i eine Unterdeterminante von D_h, und $\varkappa$ eine Zahl zwischen i und h, so giebt es eine mit Bezug auf p reguläre Determinante $D_\varkappa$ des Systems vom Grade $\varkappa$, welche D_i als Unterdeterminante enthält, und selbst als solche in D_h enthalten ist. Denn D_i wird als eine mit Bezug auf p reguläre Unterdeterminante des gesammten Systems auch eine solche reguläre Unterdeterminante desjenigen Theilsystems sein, aus welchem D_h gebildet ist, und daher findet sich, in wiederholter Anwendung des zweiten unserer Sätze, eine Determinante $D_\varkappa$ der gedachten Art, welche wenigstens in Hinsicht auf dies Theilsystem regulär ist, d. h. p in derselben Potenz $p^{\partial'_\varkappa}$ enthält, wie der grösste gemeinsame Theiler aller Unterdeterminanten $\varkappa^{\text{ten}}$ Grades von D_h. Da aber D_h regulär ist in Hinsicht auf das gesammte System, so folgt durch wiederholte Anwendung des ersten unserer Sätze, dass $\partial'_\varkappa = \partial_\varkappa$ also $D_\varkappa$ auch für das gesammte System regulär sein muss, und somit die Richtigkeit der Behauptung.

Wir nehmen nun zweitens nur $D_\varkappa$ als regulär an mit Bezug auf p. Dann ist

$$\delta_\varkappa = \partial_\varkappa.$$

*) S. Hensel a. a. O. S. 26.

Da zugleich $\sigma_{\varkappa-1} \overline{\overline{>}} \partial_{\varkappa-1}$ sein muss, folgt

$$\partial_\varkappa - \partial_{\varkappa-1} \overline{\overline{>}} \delta_\varkappa - \sigma_{\varkappa-1} \quad \text{d. i. wegen (19)} \overline{\overline{>}} \sigma^{(\varkappa)} - \delta_{\varkappa-1}.$$

Geht aber p in **sämmtlichen** Superdeterminanten von $D_{\varkappa-1}$ in der Potenz $p^{\delta^{(\varkappa)}}$ auf, so ist gewiss $\sigma^{(\varkappa)} \overline{\overline{>}} \delta^{(\varkappa)}$ und deshalb

$$\partial_\varkappa - \partial_{\varkappa-1} \overline{\overline{>}} \delta^{(\varkappa)} - \delta_{\varkappa-1}.$$

In dem besonderen Falle, in welchem $D_{\varkappa-1}$ regulär also

$$\delta_{\varkappa-1} = \partial_{\varkappa-1}$$

ist, kann $\delta^{(\varkappa)}$ nur gleich $\partial_\varkappa$ sein, und die Ungleichheit verwandelt sich in die Gleichheit

$$\partial_\varkappa - \partial_{\varkappa-1} = \delta^{(\varkappa)} - \delta_{\varkappa-1}.$$

Nun ist wegen $e_\varkappa = \frac{d_\varkappa}{d_{\varkappa-1}}$ die Potenz $p^{\partial_\varkappa - \partial_{\varkappa-1}}$ die höchste in $e_\varkappa$ aufgehende Potenz von p, man erhält also folgenden Satz:

Theilt man den grössten gemeinsamen Theiler aller Superdeterminanten einer (von Null verschiedenen) Determinante $\varkappa - 1^{\text{ten}}$ Grades durch diese letztere, so enthält der Quotient jede Primzahl p höchstens, und falls die Determinante regulär ist mit Bezug auf p, genau in derselben Potenz, wie der $\varkappa^{\text{te}}$ Elementartheiler des Systems.

Wird **drittens** umgekehrt $D_{\varkappa-1}$ als regulär mit Bezug auf p also

$$\delta_{\varkappa-1} = \partial_{\varkappa-1}$$

vorausgesetzt, so folgt, da stets $\sigma^{(\varkappa)} \overline{\overline{>}} \partial_\varkappa$ ist und wegen (19)

$$\partial_\varkappa - \partial_{\varkappa-1} \overline{\overline{<}} \sigma^{(\varkappa)} - \delta_{\varkappa-1} \overline{\overline{<}} \delta_\varkappa - \sigma_{\varkappa-1}.$$

In dem besonderen Falle, wo auch $D_\varkappa$ regulär also $\delta_\varkappa = \partial_\varkappa$ ist, muss nach dem Satze I auch $\sigma_{\varkappa-1} = \partial_{\varkappa-1}$ sein und die Ungleichheit geht in die Gleichheit

$$\partial_\varkappa - \partial_{\varkappa-1} = \delta_\varkappa - \sigma_{\varkappa-1}$$

über. Sonach ergiebt sich der weitere Satz:

Theilt man eine (von Null verschiedene) Determinante $\varkappa^{\text{ten}}$ Grades eines Systems durch den grössten gemeinsamen Theiler ihrer Subdeterminanten, so enthält der Quotient jede Primzahl p mindestens, und,

falls die Determinante regulär ist mit Bezug auf p, genau in derselben Potenz, wie der $\varkappa^{te}$ Elementartheiler des Systems*).

Als homogene lineare Funktion ihrer Subdeterminanten ist die Determinante jedenfalls durch den grössten gemeinsamen Theiler der letzteren theilbar. Demnach ist der gedachte Quotient eine ganze, durch $e_\varkappa$ theilbare Zahl.

Nun giebt es unter den Determinanten $\varkappa^{ten}$ Grades des Systems für jede Primzahl p wenigstens eine, welche in Bezug auf sie regulär ist. Werden also die gedachten Quotienten für sämmtliche jener Determinanten gebildet, so enthält einer von ihnen und folglich auch ihr grösster gemeinsamer Theiler die Primzahl p d. i. jede Primzahl genau in derselben Potenz wie $e_\varkappa$ und muss folglich gleich $e_\varkappa$ sein. Wir gelangen auf diese Weise zu der Smith'schen Definition des $\varkappa^{ten}$ Elementartheilers wieder zurück.

Drittes Capitel.

Die linearen Gleichungen.

1. Von den im Vorigen entwickelten Eigenschaften der Elementartheiler wollen wir jetzt eine Reihe von Anwendungen auf die Theorie der linearen Gleichungen und Congruenzen machen. Wir führen hier von vornherein zwei Ausdrücke ein, deren wir uns dabei zur Abkürzung bedienen. Ist a ein Zahlensystem vom Typus $m \cdot n$, so sollen diejenigen Determinanten von a, welche den höchsten Grad haben, also den Grad m oder n, jenachdem $m < n$ oder $m > n$ ist, kurz „die Determinanten" des Zahlensystems genannt werden. Ist ihr grösster gemeinsamer Theiler, also die Zahl

*) Als eine Folgerung dieses Satzes heben wir hier den folgenden hervor: Ist $D_\varkappa$ eine Unterdeterminante $\varkappa^{ten}$ Grades des Systems und gehen alle ihre Subdeterminanten durch $p^{\partial_\varkappa - 1 + \delta}$ auf, so ist $D_\varkappa$ selbst durch $p^{\partial_\varkappa + \delta}$ theilbar.

d_m resp. d_n, der Einheit gleich, so soll das Zahlensystem a ein Primsystem heissen.

Sind nun

$$A_\alpha = a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha n} x_n$$
$$(\alpha = 1, 2, \cdots m)$$

m Linearformen, deren System a vom Range r ist, so können wir statt ihrer durch die Substitution (5) vorigen Capitels zunächst m andere

$$A'_\alpha = a'_{\alpha 1} x_1 + a'_{\alpha 2} x_2 + \cdots + a'_{\alpha n} x_n$$
$$(\alpha = 1, 2, \cdots m)$$

einführen und diese dann durch die Substitution (9) ebendaselbst in ebensoviel lineare Formen

$$B_\alpha = b_{\alpha 1} y_1 + b_{\alpha 2} y_2 + \cdots + b_{\alpha n} y_n$$
$$(\alpha = 1, 2, \cdots m)$$

mit den n Unbestimmten $y_1, y_2, \cdots y_n$ verwandeln. Wählt man hierbei aber die Systeme p, q so, dass

$$b = p \cdot a \cdot q = E$$

wird, so nehmen die letzteren Formen die Gestalt an:

$$B_1 = e_1 y_1, \quad B_2 = e_2 y_2, \cdots B_r = e_r y_r, \quad B_{r+1} = 0, \cdots B_m = 0$$

und lehren, so oft $r < m$ ist, dass die Elemente des Zahlensystems

$$\begin{matrix} b_{r+1,1} & b_{r+1,2} & \cdots & b_{r+1,n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{matrix}$$

Null sind; mithin bestehen folgende Relationen:

$$a'_{\alpha 1} q_{1\beta} + a'_{\alpha 2} q_{2\beta} + \cdots + a'_{\alpha n} q_{n\beta} = 0,$$
$$(\alpha = r+1, \cdots m; \ \beta = 1, 2, \cdots n)$$

aus denen man, da die Determinante $Q = 1$ ist, für dieselben Werthe der Indices α, β

$$a'_{\alpha\beta} = 0$$

d. h. die Gleichungen

$$p_{\alpha 1} a_{1\beta} + p_{\alpha 2} a_{2\beta} + \cdots + p_{\alpha m} a_{m\beta} = 0$$
$$(\alpha = r+1, \cdots m; \ \beta = 1, 2, \cdots n)$$

erhält. Die m Elemente $a_{1\beta}, a_{2\beta}, \cdots a_{m\beta}$ sind mithin $m - r$ Bedingungsgleichungen unterworfen, deren Coefficienten, da p ein Einheitssystem ist, ein Primsystem bilden. Da hiernach

wenigstens eine Determinante des letzteren von Null verschieden ist, so lassen sich für jeden Index β aus jenen $m-r$ Gleichungen $m-r$ der Elemente $a_{1\beta}, a_{2\beta}, \cdots a_{m\beta}$ als die gleichen homogenen linearen Funktionen der übrigen darstellen, sodass auch die entsprechenden Formen $A_1, A_2, \cdots A_m$ dieselben homogenen linearen Funktionen der übrigen von ihnen werden. Man erkennt auf solche Weise den Satz: So oft der Rang r des Zahlensystems a kleiner als m ist, sind die Formen A_α nicht unabhängig von einander, vielmehr sind $m-r$ von ihnen homogene lineare Funktionen der übrigen r. Die letzteren aber sind unabhängig von einander. Gesetzt nämlich, sie seien die Formen A_1, $A_2, \cdots A_r$, so kann keine lineare Relation

$$\alpha_1 A_1 + \alpha_2 A_2 + \cdots + \alpha_r A_r = 0$$

zwischen ihnen bestehen, ohne dass sämmtliche Coefficienten $\alpha_1, \alpha_2, \cdots \alpha_r$ verschwinden; denn letztere müssten die n Gleichungen

$$a_{1\beta} \cdot \alpha_1 + a_{2\beta} \cdot \alpha_2 + \cdots + a_{r\beta} \cdot \alpha_r = 0$$
$$(\beta = 1, 2, \cdots n)$$

erfüllen, unter denen es doch, da r der Rang von a ist, r geben muss, deren Determinante von Null verschieden ist.

Wenn wir hiernach ein System von m Gleichungen

$$A_\alpha = a_\alpha \tag{1}$$
$$(\alpha = 1, 2, \cdots m)$$

betrachten, so werden, so oft $r < m$ ist, die Formen A_α nicht unabhängig von einander sein und deshalb die Constanten a_α durch genau dieselben homogenen linearen Gleichungen mit einander verbunden sein müssen, wie die Formen, damit die Gleichungen sich nicht widersprechen. Ist aber diese nothwendige Bedingung erfüllt, sind also $m-r$ der Constanten $a_1, a_2, \cdots a_m$ dieselben homogenen linearen Funktionen der übrigen, wie die entsprechenden Formen $A_1, A_2, \cdots A_m$ von den übrigen derselben, so sind ebenso viel der Gleichungen (1) die Folge der übrigen r und man braucht nur diese letzteren beizubehalten. Auf solche Weise kommt man stets auf den Fall, wo der Rang

des Systems a gleich der Anzahl der Gleichungen ist, oder auf den Fall unabhängiger Gleichungen zurück.

2. Ist insbesondere das System (1) ein überschüssiges System von Gleichungen d. h. $m > n$, so würden wir, falls $r < n$ wäre, durch diese Betrachtung sogleich auf ein unzureichendes System von $r < n$ Gleichungen mit n Unbekannten geführt, wie wir nachher es betrachten werden. Mithin dürfen wir, da r nicht $> n$ sein kann, $r = n$ voraussetzen. Ist alsdann die oben für die Auflösbarkeit der Gleichungen gefundene nothwendige Bedingung erfüllt, so werden die Gleichungen (1) stets eine (einzige) Lösung wenigstens in *rationalen* Zahlen besitzen. Denn bei derselben Wahl der Systeme p, q wie zuvor sind sie den Gleichungen

$$(2) \qquad \begin{cases} e_1 y_1 = a_1', \; e_2 y_2 = a_2', \cdots e_r y_r = a_r' \\ a_{r+1}' = 0, \; \cdots a_m' = 0 \end{cases}$$

völlig gleichbedeutend, von denen die letzteren nach der Voraussetzung erfüllt sind, während die ersteren durch ein rationales Werthsystem der y, folglich die Gleichungen (1) auch durch ein solches Werthsystem der x auflösbar sind. Ist aber das System a ein Primsystem, so ist die ausgesprochene nothwendige zugleich auch die ausreichende Bedingung dafür, dass die Gleichungen (1) eine (einzige) Lösung in *ganzen* Zahlen besitzen. Denn alsdann ist $d_n = e_1 e_2 \cdots e_n = 1$ und somit sämmtliche Elementartheiler $e_1, e_2, \cdots e_n$ der Einheit gleich, die y, welche (2) genügen, ganze Zahlen und also auch die ihnen entsprechenden x eine ganzzahlige Lösung der gegebenen Gleichungen.

Weil, so oft die nothwendige Bedingung für die Auflösbarkeit der Gleichungen (1) erfüllt ist, in dem erweiterten Systeme a:

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} & a_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & a_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} & a_m \end{matrix}$$

die Elemente gewisser $m - n$ Zeilen jedesmal die gleichen homogenen linearen Funktionen der entsprechenden Elemente

der übrigen n Reihen sind, so werden dann die Determinanten dieses Systems nothwendig verschwinden, während dies nach der Voraussetzung bei dem Systeme a nicht der Fall ist. Man überzeugt sich leicht, dass auch umgekehrt, wenn diese Bedingung erfüllt, also nicht die Determinanten des Systems a, wohl aber die Determinanten des erweiterten Systems Null sind, eine (einzige) rationale und, wenn a ein Primsystem ist, eine (einzige) ganzzahlige Lösung der Gleichungen vorhanden ist. In der That, ist z. B. die Determinante Δ der ersten n Gleichungen von Null verschieden, so findet man die Zahlen x_1, $x_2, \cdots x_n$, welche ihnen genügen, mittels der Formel

$$\Delta \cdot x_i = (-1)^{n-i+1} \cdot \begin{vmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1,i+1} & \cdots & a_{1n} & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdots & a_{n,i-1} & a_{n,i+1} & \cdots & a_{nn} & a_n \end{vmatrix}$$

und folglich wird

$$\Delta(a_{n+h} - A_{n+h}) = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} & a_n \\ a_{n+h,1} & a_{n+h,2} & \cdots & a_{n+h,n} & a_{n+h} \end{vmatrix}$$

d. i. nach der Voraussetzung

$$A_{n+h} = a_{n+h},$$

also auch den übrigen Gleichungen Genüge geleistet. Die Zahlen $x_1, x_2, \cdots x_n$ sind eindeutig bestimmt und haben rationale Werthe, deren Generalnenner nur ein Faktor von Δ sein kann. Wählt man aber für Δ nach und nach bei dieser Betrachtung sämmtliche von Null verschiedene Determinanten des Systems a, welche, so oft a ein Primsystem ist, den einzigen Faktor 1 gemein haben, so sieht man, dass jener Generalnenner in diesem Falle nur 1 sein kann, die Lösung also eine ganzzahlige ist.

Von diesem Satze machen wir sogleich Gebrauch, um folgenden anderen zu beweisen:

Wenn a ein beliebiges, ϖ ein Primsystem vom Typus $m(m+\mu)$ ist und die entsprechenden Determinanten beider sind einander proportional, jede Determinante von a also, wenn unter d der grösste

gemeinsame Theiler aller Determinanten von a verstanden wird, gleich d mal der correspondirenden Determinante von ϖ, so lässt sich auf unzweideutige Weise ein System δ vom Typus $m \cdot m$ und mit der Determinante $\Delta = d$ angeben, so beschaffen, dass

$$a = \delta \cdot \varpi \tag{3}$$

ist. In der That hat man, um diese Beziehung zu erfüllen, die $m \cdot m$ Zahlen $\delta_{\alpha\beta}$ so zu wählen, dass diejenigen von ihnen, welche die α^{te} Reihe bilden, den $m + \mu$ Gleichungen

$$a_{\alpha\beta} = \delta_{\alpha 1} \cdot \varpi_{1\beta} + \delta_{\alpha 2} \cdot \varpi_{2\beta} + \cdots + \delta_{\alpha m} \cdot \varpi_{m\beta} \tag{4}$$
$$(\beta = 1, 2, \cdots m + \mu)$$

Genüge leisten; das System der Coefficienten $\varpi_{\alpha\beta}$ dieser Gleichungen ist aber der Annahme zufolge ein Primsystem und das durch die Spalte $a_{\alpha 1}, a_{\alpha 2}, \cdots a_{\alpha, m+\mu}$ erweiterte System hat lauter verschwindende Determinanten; in der That erweist sich z. B. die Determinante

$$\begin{vmatrix} a_{\alpha 1} & \varpi_{11} & \varpi_{21} & \cdots \varpi_{m1} \\ \cdot & \cdot & \cdot & \cdot \\ a_{\alpha m} & \varpi_{1m} & \varpi_{2m} & \cdots \varpi_{mm} \\ a_{\alpha, m+1} & \varpi_{1, m+1} & \varpi_{2, m+1} & \cdots \varpi_{m, m+1} \end{vmatrix},$$

wenn sie nach den Elementen der ersten Spalte entwickelt gedacht wird, nach der Voraussetzung gleich $\frac{1}{d}$ mal der Determinante

$$\begin{vmatrix} a_{\alpha 1} & a_{11} & a_{21} & \cdots a_{m1} \\ \cdot & \cdot & \cdot & \cdot \\ a_{\alpha m} & a_{1m} & a_{2m} & \cdots a_{mm} \\ a_{\alpha, m+1} & a_{1, m+1} & a_{2, m+1} & \cdots a_{m, m+1} \end{vmatrix},$$

welche, da α einen der Werthe $1, 2, \cdots m$ bedeutet, zwei gleiche Spalten also den Werth Null hat. Dem vorigen Satze zufolge giebt es also ein System von Zahlen $\delta_{\alpha\beta}$, welche die Gleichungen (4) befriedigen; und wenn man diese für $\alpha = 1, 2, \cdots m$ und für je m Werthe β der Reihe

$$1, 2, \cdots m + \mu$$

aufstellt, so lehren sie, dass die aus diesen $m \cdot m$ Werthen $a_{\alpha\beta}$ gebildete Determinante d. i. jede Determinante des Systems

a gleich Δ mal der entsprechenden Determinante des Systems $\bar{\omega}$, folglich

$$\Delta = d$$

ist. —

3. Indem wir zu dem Falle eines unzureichenden Systems von linearen Gleichungen übergehen, betrachten wir zuerst homogene Gleichungen. Gesetzt also, man habe m Gleichungen mit $n > m$ Unbekannten

$$(5) \qquad A_\alpha = 0;$$

wir dürfen sie als unabhängig also $r = m$ voraussetzen. Verfährt man, wie im vorigen Falle, bestimmt also zwei Einheitssysteme p, q oder zwei Substitutionen (5), (9) vorigen Capitels so dass

$$p \cdot a \cdot q = E$$

wird, so gehen die Gleichungen (5) in folgendes System gleichbedeutender Gleichungen über:

$$e_1 y_1 = 0, \; e_2 y_2 = 0, \; \cdots e_m y_m = 0$$

und liefern die einzige Lösung

$$y_1 = y_2 = \cdots = y_m = 0,$$

während $y_{m+1}, \cdots y_n$ willkürlich bleiben. Nach (9) vorigen Capitels findet sich also die vollständige Auflösung der Gleichungen (5) mittels nachstehender Formel:

$$(6) \qquad x_\alpha = q_{\alpha, m+1} \cdot y_{m+1} + \cdots + q_{\alpha, n} \cdot y_n, \quad (\alpha = 1, 2, \cdots n)$$

wenn darin für $y_{m+1}, y_{m+2}, \cdots y_n$ sämmtliche ganze Zahlen gesetzt werden.

Insbesondere erhält man, indem man diese Zahlen sämmtlich gleich 0 wählt bis auf $y_{m+\beta}$, welches gleich 1 gewählt werde, $n - m$ specielle Auflösungen der Gleichungen (5):

$$(7) \qquad x_{\beta 1} = q_{1, m+\beta}, \; x_{\beta 2} = q_{2, m+\beta}, \cdots x_{\beta n} = q_{n, m+\beta}, \quad (\beta = 1, 2, \cdots n - m)$$

welche dadurch ausgezeichnet sind, dass jede andere Auflösung als eine ganzzahlige homogene lineare Funktion von ihnen dargestellt werden kann. In der That liefert die Formel (6), wenn $y_{m+\beta}$ kurz u_β genannt und $\mu = n - m$ gesetzt wird, folgende Ausdrücke:

$$(8) \qquad x_1 = \sum_{\beta=1}^{\mu} u_\beta \cdot x_{\beta 1}, \; x_2 = \sum_{\beta=1}^{\mu} u_\beta \cdot x_{\beta 2}, \; \cdots x_n = \sum_{\beta=1}^{\mu} u_\beta \cdot x_{\beta n}$$

als allgemeinste Auflösung der gegebenen Gleichungen. Aus diesem Grunde nennt man die μ besonderen Auflösungen (7) ein System fundamentaler Auflösungen; sie bilden ein Zahlensystem x vom Typus $\mu \cdot n$, von welchem man sogleich einsieht, dass es ein Primsystem ist. In der That besteht dies Zahlensystem aus den letzten μ Spalten des Systems q; da die der Einheit gleiche Determinante Q des letzteren als homogene lineare Funktion der Determinanten jener μ Spalten darstellbar ist, kann der grösste gemeinsame Theiler dieser letzteren nur der Einheit gleich sein, w. z. b. w.

Hieraus ist einzusehen, dass kein System von Fundamentalauflösungen aus weniger als μ Lösungen bestehen kann. Denn bildeten

$$y_{\beta 1}, \; y_{\beta 2}, \; \cdots y_{\beta n}$$
$$(\beta = 1, 2, \cdots \lambda)$$

ein solches Fundamentalsystem von $\lambda < \mu$ Lösungen, so würde man setzen können

$$x_{\beta\alpha} = c_{\beta 1} y_{1\alpha} + c_{\beta 2} y_{2\alpha} + \cdots + c_{\beta\lambda} y_{\lambda\alpha}$$
$$(\beta = 1, 2, \cdots \mu; \; \alpha = 1, 2, \cdots n)$$

und für das System der $x_{\beta\alpha}$ vom Typus $\mu \cdot n$ würden, obwohl es ein Primsystem ist, alle Determinanten verschwinden.

Man nennt mehrere Lösungen der Gleichungen (5) unabhängige Lösungen, wenn nicht sämmtliche Determinanten des aus ihnen gebildeten Zahlensystems gleich Null sind; z. B. bilden die fundamentalen Lösungen (7) ein System von μ unabhängigen Lösungen. Man erkennt zunächst, dass die Anzahl unabhängiger Lösungen nicht grösser als μ sein kann. Denn, sind

$$y_{\alpha 1}, \; y_{\alpha 2}, \; \cdots y_{\alpha n}$$
$$(\alpha = 1, 2, \cdots \mu + 1)$$

irgend welche $\mu + 1$ Lösungen, so bestehen den allgemeinen Formeln (8) gemäss folgende Gleichungen:

$$y_{\alpha\beta} = u_{\alpha 1} x_{1\beta} + u_{\alpha 2} x_{2\beta} + \cdots + u_{\alpha\mu} x_{\mu\beta}$$
$$(\alpha = 1, 2, \cdots \mu + 1; \; \beta = 1, 2, \cdots n)$$

und in dem Zahlensysteme vom Typus $(\mu + 1)n$ dieser Zahlen $y_{\alpha\beta}$ würden nothwendig alle Determinanten $\mu + 1^{\text{ten}}$ Grades verschwinden. Somit sind je $\mu + 1$ Lösungen von einander abhängig und die Anzahl unabhängiger Lösungen höchstens gleich μ.

Dies vorausgeschickt, seien

$$y_{\alpha 1}, \; y_{\alpha 2}, \; \cdots y_{\alpha n}$$
$$(\alpha = 1, 2, \cdots \mu)$$

irgend welche μ Lösungen der Gleichungen (5) und y ihr Zahlensystem. Aus den μn Gleichungen

$$(9) \qquad y_{\alpha\beta} = u_{\alpha 1} x_{1\beta} + u_{\alpha 2} x_{2\beta} + \cdots + u_{\alpha\mu} x_{\mu\beta}$$
$$(\alpha = 1, 2, \cdots \mu; \; \beta = 1, 2, \cdots n)$$

folgt y als das zusammengesetzte System

$$y = u \cdot x,$$

wenn man mit u, x resp. die Systeme

$$\begin{matrix} u_{11} & u_{12} & \cdots & u_{1\mu} \\ \cdot & \cdot & \cdot & \cdot \\ u_{\mu 1} & u_{\mu 2} & \cdots & u_{\mu\mu} \end{matrix} \quad \text{und} \quad \begin{matrix} x_{11} & x_{12} & \cdots & x_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ x_{\mu 1} & x_{\mu 2} & \cdots & x_{\mu n} \end{matrix}$$

vom Typus $\mu \cdot \mu$ resp. $\mu \cdot n$ bezeichnet. Für je μ Lösungen findet mithin die Beziehung statt

$$(10) \qquad y = u \cdot x.$$

Nimmt man in den Gleichungen (9) für α seine sämmtlichen, für β aber je μ Werthe der Reihe $1, 2, \cdots n$, so ist ihnen zufolge die aus den entsprechenden μ^2 Elementen $y_{\alpha\beta}$ gebildete d. h. jede Determinante von y gleich der entsprechenden Determinante von x mal der Determinante U des quadratischen Systems u.

Da das System x aber ein Primsystem ist, folgt hieraus $U = 0$, falls y ein System von einander abhängiger, U gleich dem grössten gemeinsamen Theiler aller Determinanten von y, falls y ein System unabhängiger Lösungen ist, und auch umgekehrt. Also: Jenachdem U von Null verschieden oder gleich Null ist, wird y ein System von μ unabhängigen Lösungen sein oder nicht, und im ersten Falle ist U der grösste gemeinsame Theiler aller Determinanten von y.

Aus den Betrachtungen, welche dies Ergebniss geliefert, entnimmt man ohne Mühe den weiteren Satz: In verschiedenen Systemen von μ unabhängigen Lösungen sind die einander entsprechenden Determinanten zu einander proportional.

Ist insbesondere $U = 1$, so wird y ein Primsystem sein und umgekehrt. Aus $U = 1$ folgt aber, dass u und folglich auch das reciproke System u^{-1} ganzer Zahlen

$$u'_{\alpha 1} \quad u'_{\alpha 2} \quad \cdots \quad u'_{\alpha \mu}$$
$$(\alpha = 1, 2, \cdots \mu)$$

ein Einheitssystem ist; aus (10) ergiebt sich dann

$$x = u^{-1} \cdot y$$

oder die, diese Beziehung aussprechende Formel

$$x_{\beta\alpha} = u'_{\beta 1} y_{1\alpha} + u'_{\beta 2} y_{2\alpha} + \cdots + u'_{\beta\mu} y_{\mu\alpha},$$
$$(\alpha = 1, 2, \cdots n;\ \beta = 1, 2, \cdots \mu)$$

aus welcher nach (8)

$$x_\alpha = w_1 y_{1\alpha} + w_2 y_{2\alpha} + \cdots + w_\mu y_{\mu\alpha} \tag{11}$$
$$(\alpha = 1, 2, \cdots n)$$

hervorgeht, wenn man

$$w_\gamma = u_1 u'_{1\gamma} + u_2 u'_{2\gamma} + \cdots + u_\mu u'_{\mu\gamma}$$
$$(\gamma = 1, 2, \cdots \mu)$$

setzt. Da der letzten Formel gemäss jedem Systeme ganzer Zahlen $u_1, u_2, \cdots u_\mu$ ein System ganzer Zahlen $w_1, w_2, \cdots w_\mu$ entspricht und umgekehrt, so zeigt Formel (11), dass das System y, wenn $U = 1$ ist, also jedes Primsystem von μ Lösungen ein System fundamentaler Lösungen der Gleichungen (5) ist. — Wenn umgekehrt y ein solches ist, so muss, der Formel (10) entsprechend, eine Beziehung

$$x = v \cdot y$$

stattfinden, wo v ein System ganzer Zahlen vom Typus $\mu \cdot \mu$ vorstellt. Hieraus folgt zunächst, dass nicht sämmtliche Determinanten von y verschwinden können, weil es die von x nicht thun; μ fundamentale Lösungen sind mithin auch stets unabhängige Lösungen. Ferner darf aus gleichem Grunde die Determinante V des Systems v nicht Null sein, vielmehr muss $V = 1$ und jedes System y von μ fundamentalen

Lösungen ein Primsystem also $U=1$ sein. Man hat somit den Satz:

Jenachdem $U=1$ ist oder nicht, ist das durch (10) bestimmte System y ein System von μ fundamentalen Lösungen oder nicht, oder: Damit ein System von μ Lösungen ein Fundamentalsystem sei, ist nothwendig und hinreichend, dass es ein Primsystem ist.

Hiernach ist die Formel

$$y = u \cdot x,$$

wenn darin unter u ein Einheitssystem verstanden wird, der allgemeine Ausdruck aller Systeme von μ fundamentalen Lösungen. Sei $y_0 = u_0 x$ ein bestimmtes solches System, y jedes andere, so folgt aus den beiden Gleichungen

$$y = u \cdot x, \quad y_0 = u_0 \cdot x$$

die dritte:

$$y = u u_0^{-1} \cdot y_0,$$

in welcher, da u ein beliebiges, u_0^{-1} ein bestimmtes Einheitssystem bedeutet, offenbar auch uu_0^{-1} jedes beliebige Einheitssystem vorstellt. So gewinnt man folgenden Satz:

Man erhält aus einem beliebigen Systeme y_0 von μ fundamentalen Lösungen der Gleichungen (5) die Gesammtheit solcher Systeme, wenn man in der Formel

$$y = u \cdot y_0 \tag{12}$$

für u jedes Einheitssystem vom Typus $\mu \cdot \mu$ setzt.

4. Bei der grossen Bedeutung, welche diese Sätze für die Theorie der linearen Gleichungen haben, halten wir es für angezeigt, wenigstens den Hauptsatz von der Existenz eines Systems von μ Fundamentalauflösungen noch auf eine andere Art zu beweisen, bei welcher man der allgemeinen Theorie von den Elementartheilern nicht bedarf. Eine solche Methode entnehmen wir der auf Seite 276 genannten Arbeit von Stieltjes, in welcher die Abhandlungen von Smith und theilweise auch von Frobenius über lineare Gleichungen und Congruenzen eine sehr elegante Bearbeitung gefunden haben.

Wir beginnen mit der Bemerkung, dass die Determinanten, welche aus einem Zahlensystem a vom Typus $m(m+\mu)$ sich bilden lassen, nicht sämmtlich unabhängig von einander, sondern durch gewisse Identitäten mit einander verknüpft sind. Ihre Anzahl ist offenbar

$$\frac{(\mu+1)(\mu+2)\cdots(\mu+m)}{1\cdot 2\cdots m}.$$

Bezeichnen wir nun diejenige von ihnen, welche aus den ersten m Zeilen und Spalten gebildet ist:

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{vmatrix},$$

mit Δ, ferner mit $\Delta_{i,m+\varkappa}$ diejenige, welche hieraus entsteht, wenn die i^{te} Spalte durch die $m+\varkappa^{\text{te}}$ Spalte des Systems a ersetzt wird, so erhält man $1+m\mu$ von allen jenen Determinanten, von denen sich leicht einsehen lässt, dass sie unabhängig von einander sind, d. h. dass keine für alle Werthe der Zahlen $a_{\alpha\beta}$ giltige Beziehung zwischen ihnen besteht. Dies wird man offenbar zeigen, wenn man nachweist, dass bei geeigneter Wahl der Werthe $a_{\alpha\beta}$, die freilich nicht stets ganzzahlig zu sein brauchen, jene Determinanten beliebig vorgeschriebene Werthe annehmen können. Man kann aber zunächst die Elemente von Δ so wählen, dass Δ einen (von Null verschiedenen) gegebenen Werth erhält. Ist dies geschehen, so hat man, wenn

$$\Delta_{1,m+\varkappa},\ \Delta_{2,m+\varkappa},\ \cdots\ \Delta_{m,m+\varkappa}$$

gegebene Werthe annehmen sollen, die Elemente

$$a_{1,m+\varkappa},\ a_{2,m+\varkappa},\ \cdots\ a_{m,m+\varkappa}$$

gemäss den folgenden Gleichungen:

$$\begin{aligned} A_{11}\cdot a_{1,m+\varkappa}+A_{21}\cdot a_{2,m+\varkappa}+\cdots+A_{m1}\cdot a_{m,m+\varkappa}&=\Delta_{1,m+\varkappa} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ A_{1m}\cdot a_{1,m+\varkappa}+A_{2m}\cdot a_{2,m+\varkappa}+\cdots+A_{mm}\cdot a_{m,m+\varkappa}&=\Delta_{m,m+\varkappa} \end{aligned}$$

zu bestimmen, in denen unter $A_{i\varkappa}$ das zu $a_{i\varkappa}$ adjungirte Element der Determinante Δ verstanden wird; die Werthe

$$(13)\quad a_{i,m+\varkappa} = \frac{1}{\Delta}\left(a_{i1}\Delta_{1,m+\varkappa} + a_{i2}\Delta_{2,m+\varkappa} + \cdots + a_{im}\Delta_{m,m+\varkappa}\right)$$
$$(i = 1, 2, \cdots m)$$

werden diese Gleichungen erfüllen, und indem man für $\varkappa$ jeden der Werthe $1, 2, \cdots \mu$ wählt, nehmen so in der That sämmtliche $1 + m\mu$ gedachte Determinanten beliebig vorgeschriebene Werthe an. Die übrigen Determinanten des Systems a sind aber nun durch diese $1 + m\mu$ zugleich mitbestimmt. Denn, ist Δ' diejenige, in welcher die Spalten $\mu_1, \mu_2, \cdots \mu_h$ von Δ fehlen und durch die Spalten $m + \lambda_1, m + \lambda_2, \cdots m + \lambda_h$ des Systems a ersetzt sind, so ergiebt sich, wenn man für die Elemente der letzteren ihre Ausdrücke (13) einführt, nach den einfachsten Determinantensätzen folgende Beziehung:

$$(14)\qquad \Delta' = \frac{\pm 1}{\Delta^{h-1}} \begin{vmatrix} \Delta_{\mu_1,m+\lambda_1} & \Delta_{\mu_1,m+\lambda_2} & \cdots & \Delta_{\mu_1,m+\lambda_h} \\ \cdot & \cdot & \cdot & \cdot \\ \Delta_{\mu_h,m+\lambda_1} & \Delta_{\mu_h,m+\lambda_2} & \cdots & \Delta_{\mu_h,m+\lambda_h} \end{vmatrix}.$$

Dies vorausgeschickt, sei nun ein System von m unabhängigen Gleichungen (5) mit $n = m + \mu$ Unbekannten gegeben, und wir wollen annehmen, unter den von Null verschiedenen Determinanten des Systems a habe die Determinante Δ den kleinsten Werth. Aus den Gleichungen lassen sich dann die Unbekannten $x_1, x_2, \cdots x_m$ durch die übrigen mittels der Formel

$$(15)\quad x_i = -\frac{1}{\Delta}\left(\Delta_{i,m+1}x_{m+1} + \Delta_{i,m+2}x_{m+2} + \cdots + \Delta_{i,n}x_n\right)$$

ausdrücken; um sämmtliche ganzzahlige Auflösungen der Gleichungen zu finden, wird man daher die sonst willkürlichen Werthe $x_{m+1}, x_{m+2}, \cdots x_n$ so als ganze Zahlen zu bestimmen haben, dass auch $x_1, x_2, \cdots x_m$ ganzzahlig werden. In dem besonderen Falle, wo sämmtliche Determinanten $\Delta_{i,m+\varkappa}$, folglich nach (14) überhaupt sämmtliche Determinanten von a durch Δ theilbar sind, bleiben mithin $x_{m+1}, x_{m+2}, \cdots x_n$ völlig willkürliche ganze Zahlen und die vorige Formel liefert die vollständige Auflösung der Gleichungen (5), indem man für $x_{m+1}, x_{m+2}, \cdots x_n$ sämmtliche ganzzahligen Werthe einsetzt. Ist aber z. B. $\Delta_{1,m+1}$ nicht theilbar durch Δ, so führe man in die Gleichungen (5) durch die unimodulare Substitution

$$x_1 = x_1' - c x'_{m+1},$$

in welcher c eine sogleich näher zu bestimmende ganze Zahl bezeichnet, neue Variabeln ein; die Gleichungen $A_\alpha = 0$ gehen dadurch in andere $B_\alpha = 0$ über und jeder ganzzahligen Auflösung des ersteren Systems entspricht eine solche des neuen und umgekehrt. Da das System a dabei durch das folgende

$$\begin{matrix} a_{11} & \cdots & a_{1,m} & a_{1,m+1} - c a_{11} & \cdots & a_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & \cdots & a_{m,m} & a_{m,m+1} - c a_{m1} & \cdots & a_{m,m+\mu} \end{matrix}$$

ersetzt wird, so geht die Determinante $\Delta_{1,m+1}$ offenbar in $\Delta_{1,m+1} - c\Delta$ über und die ganze Zahl c kann so gewählt werden, dass dieser neue Werth von Null verschieden aber kleiner als Δ ausfällt. Alsdann kann man das gleiche Verfahren wiederholen, muss so aber, da jedesmal die Minimaldeterminante des Systems verringert wird, nach einer endlichen Anzahl von Wiederholungen auf den Fall kommen, dass sämmtliche Determinanten des Systems durch eine von ihnen theilbar sind. Die Variabeln des so an Stelle des gegebenen tretenden Systems von Gleichungen sind dann, dem ersten Falle entsprechend, homogene lineare ganzzahlige Funktionen von μ willkürlichen ganzen Zahlen, und, da die ursprünglichen Variabeln selbst eben solche Funktionen von jenen sind, so gilt von ihnen genau das Gleiche. Die allgemeinste Lösung der Gleichungen (5) hat also die Gestalt, welche in den Formeln (8) auf anderem Wege für sie gefunden worden ist. Hiermit ist die Existenz eines Systems von μ fundamentalen Auflösungen festgestellt.

5. Bevor wir uns jetzt von den homogenen zu den nicht homogenen Gleichungen wenden, ziehen wir aus der fundamentalen Beziehung (15) des vorigen Capitels, indem wir darin $r = m < n$ voraussetzen, einen wichtigen weiteren Schluss.

Schreiben wir dieselbe in der Gestalt:

$$a = p^{-1} \cdot E \cdot q^{-1}$$

und nehmen als die Systeme p^{-1} und q^{-1} die beiden folgenden an:

$$\begin{matrix} p'_{11} & p'_{12} & \cdots & p'_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ p'_{m1} & p'_{m2} & \cdots & p'_{mm} \end{matrix} \qquad \begin{matrix} q'_{11} & q'_{12} & \cdots & q'_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ q'_{n1} & q'_{n2} & \cdots & q'_{nn}, \end{matrix}$$

so besteht die allgemeine Gleichung

$$a_{\alpha\beta} = e_1 \cdot p'_{\alpha 1} q'_{1\beta} + e_2 \cdot p'_{\alpha 2} q'_{2\beta} + \cdots + e_m \cdot p'_{\alpha m} q'_{m\beta}$$
$$(\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots n)$$

und demnach folgende Determinantenrelation:

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{m1} & \cdots & a_{mn} \\ q'_{m+1,1} & \cdots & q'_{m+1,n} \\ \cdot & \cdot & \cdot \\ q'_{n1} & \cdots & q'_{nn} \end{vmatrix} = \begin{vmatrix} e_1 p'_{11} & \cdots & e_m p'_{1m} & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ e_1 p'_{m1} & \cdots & e_m p'_{mm} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{vmatrix} \cdot \begin{vmatrix} q'_{11} & \cdots & q'_{1n} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ q'_{n1} & \cdots & q'_{nn} \end{vmatrix}.$$

Da p'^{-1}, q'^{-1} Einheitssysteme sind, erhält die zur Linken stehende Determinante den Werth $e_1 e_2 \cdots e_m = d_m$ und wir gelangen zu folgendem Satze:

Ist a ein Zahlensystem vom Typus $m(m+\mu)$, dessen Determinanten nicht sämmtlich verschwinden, so kann man demselben ein *complementäres* System vom Typus $\mu(m+\mu)$ anfügen, so beschaffen, dass die Determinante des aus beiden gebildeten quadratischen Systems vom Typus $(m+\mu)(m+\mu)$ gleich dem grössten gemeinsamen Theiler aller Determinanten von a, also, wenn a ein Primsystem ist, gleich 1 wird.

Diesem allgemeinen Resultate gemäss kann man insbesondere, wenn $\mu+1$ Zahlen

$$a_{11}\, a_{12} \cdots a_{1,\mu+1}$$

ohne gemeinsamen Theiler gegeben sind, ihnen μ Reihen von $\mu+1$ Zahlen

$$\begin{matrix} q'_{21} & q'_{22} & \cdots & q'_{2,\mu+1} \\ \cdot & \cdot & \cdot & \cdot \\ q'_{\mu+1,1} & q'_{\mu+1,2} & \cdots & q'_{\mu+1,\mu+1} \end{matrix}$$

anfügen, so beschaffen, dass die Determinante aller $(\mu + 1)^2$ Zahlen der Einheit gleich wird, oder man kann ein Einheitssystem vom Typus $(\mu + 1) \cdot (\mu + 1)$ bilden, welches die gegebenen Zahlen als seine erste Zeile enthält. Denkt man sich die Determinante nach den Elementen der ersten Zeile entwickelt und nennt $A_{i\varkappa}$ das zu $a_{i\varkappa}$ adjungirte Element derselben, so erhält man die Gleichung

$$a_{11} A_{11} + a_{12} A_{12} + \cdots + a_{1,\mu+1} A_{1,\mu+1} = 1.$$

Sind also $a_{11}, a_{12}, \cdots a_{1,\mu+1}$ Zahlen ohne gemeinsamen Theiler, so ist die Gleichung

$$(16) \qquad a_{11} x_1 + a_{12} x_2 + \cdots + a_{1,\mu+1} x_{\mu+1} = 1$$

in ganzen Zahlen $x_1, x_2, \cdots x_{\mu+1}$ auflösbar. Gleiches gilt jedenfalls auch von der Gleichung

$$(17) \qquad a_{11} x_1 + a_{12} x_2 + \cdots + a_{1,\mu+1} x_{\mu+1} = d,$$

wenn d grösster gemeinsamer Theiler der Coefficienten ist.

Die Aufgabe, alle Einheitssysteme der letzteren Art zu finden, ist allgemein zuerst von Hermite gelöst worden*). Wir beschäftigen uns aber sogleich mit der andern, von welcher sie nur den einfachsten Fall darstellt: Zu einem gegebenen Primsysteme a vom Typus $m(m + \mu)$ sämmtliche complementäre zu finden, so beschaffen, dass das Gesammtsystem vom Typus $(m + \mu) \cdot (m + \mu)$ eine der Einheit gleiche Determinante hat. Da ein solch complementäres System durch die Betrachtungen, die uns zum obigen Satze

*) S. Liouville's Journ. des Math. XIV p. 21—30. Dieselbe Aufgabe unter anderer Einkleidung hat Jacobi in einer nachgelassenen Abhandlung: „über die Auflösung der Gleichung

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = f \cdot u\text{“}$$

im Journ. f. Math. 69 S. 1 auf vier verschiedene Weisen behandelt. Für $\mu = 2$ gab Eisenstein die Lösung der Aufgabe in seinen „Allgemeine Untersuch. üb. die Formen 3. Gr. mit 3 Var., welche der Kreistheilung ihre Entstehung verdanken“, J. f. Math. 28.

geführt haben, unmittelbar geliefert wird, handelt es sich nur darum, aus einem solchen Systeme sämmtliche übrigen herzuleiten. Sei das erstere Gesammtsystem:

$$\gamma = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{m,m+\mu} \\ \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_{\mu 1} & \gamma_{\mu 2} & \cdots & \gamma_{\mu,m+\mu} \end{matrix}$$

jedes andere:

$$x = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{m,m+\mu} \\ x_{11} & x_{12} & \cdots & x_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ x_{\mu 1} & x_{\mu 2} & \cdots & x_{\mu,m+\mu} \end{matrix}.$$

Aus dem Schlusssatze von nr. 2, der, wie von selbst einleuchtet, auch in dem Grenzfalle $m = n$ seine Geltung behält, schliesst man sogleich das Bestehen einer Gleichung

$$x = e \cdot \gamma,$$

worin e ein Einheitssystem:

$$\begin{matrix} e_{11} & e_{12} & \cdots & e_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ e_{m+\mu,1} & e_{m+\mu,2} & \cdots & e_{m+\mu,m+\mu} \end{matrix}$$

ist. Daraus folgt

$$e = x \cdot \gamma^{-1},$$

wo γ^{-1} das zu γ reciproke System bezeichnet, dessen Elemente

$$\begin{matrix} A_{11} & A_{21} & \cdots & A_{m1}, & \Gamma_{11} & \cdots & \Gamma_{\mu 1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ A_{1,m+\mu} & A_{2,m+\mu} & \cdots & A_{m,m+\mu}, & \Gamma_{1,m+\mu} & \cdots & \Gamma_{\mu,m+\mu} \end{matrix}$$

heissen mögen. Demnach bestehen die beiden allgemeinen Formeln

$$e_{\alpha\beta} = a_{\alpha 1} A_{\beta 1} + a_{\alpha 2} A_{\beta 2} + \cdots + a_{\alpha,m+\mu} A_{\beta,m+\mu}$$
$$(\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots m)$$

und

$$e_{\alpha,m+\gamma} = a_{\alpha 1}\Gamma_{\gamma 1} + a_{\alpha 2}\Gamma_{\gamma 2} + \cdots + a_{\alpha,m+\mu}\Gamma_{\gamma,m+\mu}$$
$$(\alpha = 1, 2, \cdots m;\ \gamma = 1, 2, \cdots \mu)$$

d. i. nach den bekannten Beziehungen zwischen den Elementen einer Determinante und ihren adjungirten Elementen

$$e_{\alpha\alpha} = 1, \quad e_{\alpha\beta} = 0, \quad \text{wenn } \alpha \gtrless \beta, \quad e_{\alpha,m+\gamma} = 0.$$

Das System e hat daher folgende Gestalt:

$$\begin{matrix} 1 & \cdots 0 & 0 & 0 \cdots 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \cdots 1 & 0 & 0 \cdots 0 \\ e_{m+1,1} & \cdots e_{m+1,m} & e_{m+1,m+1} & \cdots e_{m+1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ e_{m+\mu,1} & \cdots e_{m+\mu,m} & e_{m+\mu,m+1} & \cdots e_{m+\mu,m+\mu}. \end{matrix}$$

Die in den letzten μ Zeilen und Spalten befindlichen Elemente $e_{m+\alpha,m+\beta}$ bilden eine unimodulare Determinante μ^{ten} Grades, in welcher $\varepsilon_{m+\alpha,m+\beta}$ das zu $e_{m+\alpha,m+\beta}$ adjungirte Element sei. Wenn man dann

$$(18) \qquad \eta_{\beta\gamma} = \varepsilon_{m+1,m+\beta} \cdot e_{m+1,\gamma} + \cdots + \varepsilon_{m+\mu,m+\beta} \cdot e_{m+\mu,\gamma}$$
$$(\beta = 1, 2, \cdots \mu;\ \gamma = 1, 2, \cdots m)$$

setzt, so folgt sogleich

$$e_{m+\alpha,m+1} \cdot \eta_{1\gamma} + \cdots + e_{m+\alpha,m+\mu} \cdot \eta_{\mu\gamma} = e_{m+\alpha,\gamma}$$
$$(\alpha = 1, 2, \cdots \mu;\ \gamma = 1, 2, \cdots m)$$

und man erkennt hieraus, dass das System e aus folgenden beiden anderen:

$$e_\mu = \begin{matrix} 1\ 0 \cdots 0 & 0 & \cdots 0 \\ \cdot & \cdot & \cdot \\ 0\ 0 \cdots 1 & 0 & \cdots 0 \\ 0\ 0 \cdots 0 & e_{m+1,m+1} & \cdots e_{m+1,m+\mu} \\ \cdot & \cdot & \cdot \\ 0\ 0 \cdots 0 & e_{m+\mu,m+1} & \cdots e_{m+\mu,m+\mu}, \end{matrix}$$

$$\eta = \begin{matrix} 1 & 0 & \cdots 0 & 0\ 0 \cdots 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots 1 & 0\ 0 \cdots 0 \\ \eta_{11} & \eta_{12} & \cdots \eta_{1m} & 1\ 0 \cdots 0 \\ \cdot & \cdot & \cdot & \cdot \\ \eta_{\mu 1} & \eta_{\mu 2} & \cdots \eta_{\mu m} & 0\ 0 \cdots 1 \end{matrix}$$

zusammengesetzt ist. **Mithin hat man**

$$x = e_\mu \cdot \eta \cdot \gamma$$

und man findet die allgemeinste Auflösung der Aufgabe mittels der, diese Beziehung ausdrückenden Formel:

$$x_{\alpha\beta} = \sum_{\varkappa=1}^{\mu} \xi_{\alpha,\varkappa}(\gamma_{\varkappa\beta} + \eta_{\varkappa 1} a_{1\beta} + \cdots + \eta_{\varkappa m} a_{m\beta}),$$
$$(\alpha = 1, 2, \cdots \mu;\ \beta = 1, 2, \cdots m + \mu)$$

in welcher die μ^2 Zahlen $\xi_{\alpha,\varkappa} = e_{m+\alpha, m+\varkappa}$ ein Einheitssystem bilden, während die $\mu \cdot m$ Zahlen $\eta_{\varkappa\lambda}$ den Formeln (18) zufolge ganz willkürliche ganze Zahlen sind, da die in diesen Formeln auftretenden $\mu \cdot m$ Zahlen $e_{m+\varkappa,\lambda}$ gleichfalls willkürliche ganze Zahlen bedeuten.

6. Wenn wir nun zu den linearen Gleichungen zurückkehrend, unter b ein System von μ unabhängigen Auflösungen

$$b_{\beta 1}\ b_{\beta 2} \cdots b_{\beta n} \qquad (\beta = 1, 2, \cdots \mu) \tag{19}$$

der m Gleichungen

$$A_\alpha = 0 \qquad (\alpha = 1, 2, \cdots m) \tag{5}$$

verstehen, so bildet dasselbe zusammen mit dem Systeme a ein quadratisches System vom Typus $(m + \mu) \cdot (m + \mu)$:

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{m,m+\mu} \\ b_{11} & b_{12} & \cdots & b_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ b_{\mu 1} & b_{\mu 2} & \cdots & b_{\mu,m+\mu}, \end{matrix}$$

dessen Elemente durch die allgemeine Formel

$$a_{\alpha 1} b_{\beta 1} + a_{\alpha 2} b_{\beta 2} + \cdots + a_{\alpha,m+\mu} b_{\beta,m+\mu} = 0$$

mit einander verbunden sind. Demgemäss stellen offenbar die Elemente des Systems a, nämlich die Werthe

$$a_{\alpha 1}\ a_{\alpha 2} \cdots a_{\alpha n} \qquad (\alpha = 1, 2, \cdots m) \tag{20}$$

ein System von m Auflösungen der μ Gleichungen

$$(21) \qquad b_{\beta 1} \cdot y_1 + b_{\beta 2} \cdot y_2 + \cdots + b_{\beta n} \cdot y_n = 0$$
$$(\beta = 1, 2, \cdots \mu)$$

vor, welche wir kurz die zu den Gleichungen $A_\alpha = 0$ adjungirten Gleichungen $B_\beta = 0$ nennen wollen, und zwar ein System von m unabhängigen Auflösungen, da die Determinanten des Systems a nicht sämmtlich verschwinden. Diese Reciprocität zwischen den Systemen a und b spricht sich auch noch in einem Satze aus, den wir hier zunächst anfügen müssen. Denkt man sich die Determinante C des quadratischen Systems nach den Determinanten ihrer ersten m Zeilen entwickelt, so dass nach (13) des ersten Capitels

$$C = \sum_{\varrho\sigma\tau\cdots}' C^{(m)}_{12\cdots m,\, \varrho\sigma\tau\cdots} \cdot \overline{C}^{(m)}_{12\cdots m,\, \varrho\sigma\tau\cdots}$$

ist, so ist dem ersten Faktor unter dem Summenzeichen, der eine beliebige Determinante des Systems a bezeichnet, als zweiter Faktor offenbar diejenige Determinante des Systems b zugesellt, welche aus den im ersten nicht vorkommenden Spalten gebildet ist, und die wir deshalb die complementäre Determinante von b nennen wollen. Der zu beweisende Satz lautet dann: Die Determinanten des Systems der Coefficienten in den Gleichungen

$$A_\alpha = 0$$

sind proportional den complementären Determinanten im System der Coefficienten der adjungirten Gleichungen

$$B_\beta = 0.$$

Um ihn zu beweisen, schicken wir die Bemerkung voraus, dass, da die letzteren Coefficienten die Elemente irgend eines Systems von μ unabhängigen Auflösungen der ersteren Gleichungen sind, nach einem in nr. 3 ausgesprochenen Satze aber die entsprechenden Determinanten verschiedener solcher Systeme unter sich proportional sind, es offenbar genügen wird, den behaupteten Satz für ein bestimmtes System von μ unabhängigen Lösungen zu beweisen. Nun wähle man die $\mu(m + \mu)$ Zahlen

$$\gamma_{\beta 1},\ \gamma_{\beta 2} \cdots \gamma_{\beta, m+\mu}$$
$$(\beta = 1, 2, \cdots \mu)$$

nach nr. 5 so, dass die Determinante

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{m,m+\mu} \\ \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1,m+\mu} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_{\mu 1} & \gamma_{\mu 2} & \cdots & \gamma_{\mu,m+\mu} \end{vmatrix}$$

dem grössten gemeinsamen Theiler d aller Determinanten von a gleich wird, und bezeichne mit $\Gamma_{\alpha\beta}$ das zu $\gamma_{\alpha\beta}$ adjungirte Element in dieser Determinante. Da alsdann die Identität stattfindet

$$a_{\alpha 1}\cdot\Gamma_{\beta 1}+a_{\alpha 2}\cdot\Gamma_{\beta 2}+\cdots+a_{\alpha,m+\mu}\cdot\Gamma_{\beta,m+\mu}=0,$$
$$(\alpha=1,2,\cdots m;\ \beta=1,2,\cdots\mu)$$

so bezeichnet das System Γ der $\mu(m+\mu)$ Zahlen

$$\Gamma_{\beta 1},\ \Gamma_{\beta 2},\ \cdots\ \Gamma_{\beta,m+\mu}$$
$$(\beta=1,2,\cdots\mu)$$

ein System von μ Lösungen der Gleichungen (5); ferner ist nach Formel (15) des ersten Capitels jede aus diesem System gebildete Determinante vom Grade μ proportional, nämlich gleich $d^{\mu-1}$ mal der complementären Determinante des Systems a; da letztere nicht sämmtlich verschwinden, ist Γ ein System von unabhängigen Lösungen, und somit der Satz bewiesen*).

7. Nach dem Satze, mit dessen Beweis wir nr. 2 beschlossen, giebt es, wenn a und ϖ zwei gegebene Systeme vom Typus $m(m+\mu)$, das letztere ein Primsystem bedeuten, deren entsprechende Determinanten einander proportional sind, ein einziges System δ vom Typus $m\cdot m$ so beschaffen, dass

$$a=\delta\cdot\varpi, \tag{22}$$

die Determinante Δ also gleich dem grössten gemeinsamen Theiler d aller Determinanten von a ist. Wir wollen jetzt die Aufgabe lösen, alle Systeme δ, ϖ vom Typus $m\cdot m$ resp. $m(m+\mu)$, das letztere als Primsystem, zu be-

*) Einen andern Beweis schöpft Stieltjes in der angeführten Schrift aus den in nr. 4 gegebenen Formeln. S. auch Frobenius Journ. f. Math. 82 S. 237.

stimmen, welche bei gegebenem System a der Gleichung (22) genügen. Dies kann auf Grund des Satzes der vorigen nr. leicht ausgeführt werden. In der That giebt es zunächst, wie wir wissen, unendlich viel Systeme von μ unabhängigen Lösungen der Gleichungen (5); sei das System b der $\mu(m+\mu)$ Zahlen

$$b_{\beta 1}\ b_{\beta 2} \cdots b_{\beta, m+\mu}$$
$$(\beta = 1, 2, \cdots \mu)$$

ein solches. Dem erwähnten Satze zufolge sind die Determinanten von a den complementären Determinanten von b proportional. Denkt man sich nun die Gleichungen

$$B_\beta = 0$$
$$(\beta = 1, 2, \cdots \mu)$$

aufgestellt, und bezeichnet mit ϖ_0 irgend eines der unendlich vielen Systeme von m Fundamentalauflösungen

$$\varpi_{\alpha 1}\ \varpi_{\alpha 2} \cdots \varpi_{\alpha, m+\mu}$$
$$(\alpha = 1, 2, \cdots m)$$

dieser Gleichungen, so ist ϖ_0 ein Primsystem vom Typus $m(m+\mu)$, dessen Determinanten den complementären Determinanten von b und folglich den entsprechenden Determinanten von a nach demselben Satze proportional sind. Nach nr. 2 giebt es dann ein einziges System δ_0 vom Typus $m \cdot m$, welches mit ϖ_0 zugleich die Gleichung (22) erfüllt. Somit erweist sich also zunächst die gestellte Aufgabe als lösbar. Aus einer Lösung

$$a = \delta_0 \cdot \varpi_0$$

dieser Gleichung gehen aber alle übrigen sehr einfach hervor. Die entsprechenden Determinanten der beiden Primsysteme ϖ und ϖ_0 müssen nämlich offenbar einander gleich sein, und demnach giebt es nach nr. 2 ein System e vom Typus $m \cdot m$, für welches

$$\varpi = e \cdot \varpi_0$$

ist, während seine Determinante $\varepsilon = 1$ ist; demnach wird

$$\delta \cdot \varpi = \delta e \cdot \varpi_0 = \delta_0 \cdot \varpi_0$$

also, wie ebenfalls aus nr. 2 folgt, $\delta e = \delta_0$ und, da e ein Einheitssystem ist, auch umgekehrt $\delta = \delta_0 \cdot e^{-1}$. Die allgemeinste

Auflösung der Gleichung (22) lautet also, wenn δ_0, ϖ_0 eine bestimmte Auflösung, e aber irgend ein Einheitssystem vom Typus $m \cdot m$ ist,

$$\delta = \delta_0 \cdot e^{-1}, \quad \varpi = e \cdot \varpi_0.$$

Mit Hilfe dieses Resultates lösen wir nun eine andere Aufgabe, die sich mehrfach in der Folge uns darbieten wird. Es handelt sich darum, alle Systeme eines gegebenen Typus aufzustellen, deren Determinanten gegebene (nicht sämmtlich verschwindende) Werthe haben*).

Das gesuchte System sei vom Typus $\mu(m+\mu)$. Wir bemerken vor Allem, dass die Werthe seiner Determinanten nicht völlig willkürlich angenommen werden dürfen, da sie, wie in nr. 4 auseinandergesetzt, theilweise abhängig von einander sind.

Man darf, wenn das System ein ganzzahliges sein soll, die dort mit $\Delta, \Delta_{i,m+\varkappa}$ bezeichneten Determinanten offenbar nur mit der Einschränkung willkürlich wählen, dass entsprechend der Formel (14) auch sämmtliche übrigen Determinanten Δ' ganze Werthe erhalten. Es wird mithin vorausgesetzt, dass die gegebenen Werthe für die Determinanten des gesuchten Systems a dieser Bedingung entsprechen. Alsdann gestattet die Aufgabe unendlich viele Auflösungen. In der That können wir zuerst die Elemente $\alpha_{i\varkappa}$ in den ersten μ Zeilen und Spalten eines Systems vom angegebenen Typus so wählen, dass die Determinante $|\alpha_{i\varkappa}|$ einen der vorgeschriebenen, von Null verschiedenen Werthe erhalte, den wir mit Δ bezeichnen wollen. Darauf lassen sich

$$\alpha_{1,\mu+\varkappa}\ \alpha_{2,\mu+\varkappa} \cdots \alpha_{\mu,\mu+\varkappa} \qquad (\varkappa = 1, 2, \cdots m) \tag{23}$$

nach dem Vorbilde der Formel (13) so wählen, dass auch sämmtliche übrige Determinanten die vorgeschriebenen Werthe erhalten. Freilich werden dabei die Zahlen (23) nicht noth-

*) Diese Aufgabe ist zuerst von Gauss für den Typus $2 \cdot 3$ im art. 279 seiner Disqu. Arithm. (vgl. Cap. 2 nr. 7 des ersten Abschnittes) und für den Typus $2 \cdot 4$ im art. 236 ders. gelöst worden. Die im Text gegebene Lösung ist der mehrfach genannten Schrift von Stieltjes entnommen.

wendig ganze Werthe erhalten. Wenn man jedoch sämmtliche Elemente des so erhaltenen Systems mit $'\Delta$ multiplicirt, so bekommt man ein System lauter ganzer Zahlen, dessen Determinanten den vorgeschriebenen Werthen offenbar proportional sind. Nennt man dies System $\mathfrak{a}$ und bestimmt, wie in der vorigen Aufgabe, ein Primsystem ϖ_0 vom gleichen Typus und ein System δ_0 vom Typus $\mu \cdot \mu$ so, dass die Gleichung

$$\mathfrak{a} = \delta_0 \varpi_0$$

erfüllt wird, so sind die vorgeschriebenen Werthe, weil den Determinanten von $\mathfrak{a}$, auch den entsprechenden Determinanten von ϖ_0 proportional, und zwar, da ϖ_0 ein Primsystem ist, sind sie, durch ihren grössten gemeinsamen Theiler d dividirt, den letzteren gleich. Ist mithin δ ein System vom Typus $\mu \cdot \mu$, dessen Determinante Δ gleich d ist, wie es offenbar solcher Systeme unendlich viele giebt, so müssen nothwendigerweise in dem Systeme

$$a = \delta \cdot \varpi_0 \tag{24}$$

die Determinanten die vorgeschriebenen Werthe haben. Und da umgekehrt, wenn a ein solches System ist, es nach nr. 2 ein bestimmtes System δ vom Typus $\mu \cdot \mu$ mit der Determinante $\Delta = d$ giebt, für welches $a = \delta \cdot \varpi_0$ wird, so liefert die Formel (24) sämmtliche Lösungen der Aufgabe, wenn man darin für δ sämmtliche Systeme der angegebenen Beschaffenheit setzt.

8. Wir heben den besonderen Fall dieser Aufgabe hervor, in welchem $m = 1$ ist, also sämmtliche Systeme vom Typus $\mu(\mu + 1)$ zu finden sind, deren $\mu + 1$ Determinanten $\Delta_1, \Delta_2, \cdots \Delta_{\mu+1}$*) vorgeschriebene Werthe $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$ haben sollen. Für diesen wichtigsten Fall soll hier die Lösung noch mitgetheilt werden, welche Hermite dafür gegeben hat**).

Jedes System

---

*) Wir wollen dabei mit Δ_i diejenige Determinante des Systems bezeichnen, welche die i^{te} Spalte desselben nicht enthält.

**) S. Journ. f. Math. 40 S. 264.

(25) $$x_{\alpha 1}\ x_{\alpha 2} \cdots x_{\alpha,\mu+1} \quad (\alpha = 1, 2, \cdots \mu)$$

der verlangten Art bildet zusammen mit $\mu + 1$ beliebigen Elementen eine Determinante $\mu + 1^{\text{ten}}$ Grades, in welcher die vorgeschriebenen Werthe zu jenen Elementen adjungirt sind: mithin bestehen die μ Gleichungen:

(26) $$\alpha_1 \cdot x_{\beta 1} + \alpha_2 \cdot x_{\beta 2} + \cdots + \alpha_{\mu+1} \cdot x_{\beta,\mu+1} = 0 \quad (\beta = 1, 2, \cdots \mu)$$

d. h. die Elemente des gesuchten Systems sind μ Lösungen der Gleichung

(27) $$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_{\mu+1} x_{\mu+1} = 0;$$

sie sind auch unabhängige Lösungen derselben, wenn, wie wir voraussetzen, nicht sämmtliche Zahlen $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$, z. B. α_1 nicht gleich Null sind. Umgekehrt, wenn die Elemente (25) μ unabhängige Lösungen dieser Gleichung vorstellen, so folgt aus den μ Identitäten (26), dass die Determinanten $\varDelta_1$, $\varDelta_2, \cdots \varDelta_{\mu+1}$ proportional sind zu $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$ resp. Nun lassen sich leicht solche μ unabhängige Lösungen von (27) aufstellen. Z. B., wenn $\delta_\varkappa$ den grössten gemeinsamen Theiler der Zahlen $\alpha_1, \alpha_2, \cdots \alpha_\varkappa$ bezeichnet, sodass $\delta_{\mu+1}$ mit dem grössten gemeinsamen Theiler d sämmtlicher Zahlen $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$ identisch ist, erhält man eine Lösung der Gleichung (27), wenn man $x_1, x_2, \cdots x_{\varkappa-1}$ der Gleichung

(28) $$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_{\varkappa-1} x_{\varkappa-1} = -\,\delta_{\varkappa-1} \cdot \frac{\alpha_\varkappa}{\delta_\varkappa}\ {}^{*)}$$

gemäss wählt, alsdann

$$x_\varkappa = \frac{\delta_{\varkappa-1}}{\delta_\varkappa}$$

und die übrigen x gleich Null setzt. Auf solche Weise bilden wir μ Lösungen, die wir folgendermassen bezeichnen wollen:

(29) $$\begin{cases} \xi_{11} & \frac{\delta_1}{\delta_2} & 0 & \cdots 0 & 0 \\ \xi_{21} & \xi_{22} & \frac{\delta_2}{\delta_3} & \cdots 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \xi_{\mu 1} & \xi_{\mu 2} & & \cdots \xi_{\mu\mu} & \frac{\delta_\mu}{\delta_{\mu+1}} \end{cases}$$

*) Dass solche Wahl möglich ist, würde aus dem Satze (17) in nr. 5

und deren System das System ξ heisse. Zur näheren Feststellung der $\xi_{\alpha\beta}$ wähle man die 2μ ganzen Zahlen

$$\varkappa_1, \varkappa_2, \cdots \varkappa_\mu; \lambda_1, \lambda_2, \cdots \lambda_\mu$$

gemäss den Gleichungen

$$\varkappa_\beta \cdot \alpha_{\beta+1} + \lambda_\beta \cdot \delta_\beta = \delta_{\beta+1}, \quad (\beta = 1, 2, \cdots \mu)$$

was bekannterweise geschehen kann, da $\delta_{\beta+1}$ der grösste gemeinsame Theiler von δ_β, $\alpha_{\beta+1}$ ist, und setze

$$\xi_{\beta\gamma} = - \varkappa_{\gamma-1}\lambda_\gamma\lambda_{\gamma+1} \cdots \lambda_{\beta-1} \cdot \frac{\alpha_{\beta+1}}{\delta_{\beta+1}} \text{ für } \gamma < \beta$$

$$\xi_{\beta\beta} = - \varkappa_{\beta-1} \cdot \frac{\alpha_{\beta+1}}{\delta_{\beta+1}},$$

alsdann erfüllen die Werthe (29), wie man sich sogleich überzeugt, thatsächlich die Gleichung (27) sowohl wie (28). Nun sind die so aufgestellten μ Lösungen der letzteren unabhängige Lösungen, denn diejenige Determinante von ξ, welche die erste Spalte nicht enthält, ist gleich

$$\frac{\delta_1}{\delta_2} \cdot \frac{\delta_2}{\delta_3} \cdots \frac{\delta_{\mu-1}}{\delta_\mu} \cdot \frac{\delta_\mu}{\delta_{\mu+1}} = \frac{\delta_1}{d} = \frac{\alpha_1}{d}$$

also von Null verschieden. In Folge davon sind die Determinanten von ξ proportional resp. zu $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$, und da die erste von ihnen gleich $\frac{\alpha_1}{d}$, so sind sie sämmtlich gleich

$$\frac{\alpha_1}{d}, \frac{\alpha_2}{d}, \cdots \frac{\alpha_{\mu+1}}{d}$$

d. h. Zahlen ohne gemeinsamen Theiler, und das System ξ ist also ein Primsystem. Wird also wieder unter δ ein System vom Typus $\mu \cdot \mu$ verstanden, dessen Determinante gleich d ist, so wird das System

$$a = \delta \cdot \xi$$

ein System der gesuchten Art, und jedes System dieser Art vorstellen, wenn für δ darin jedes System der bezeichneten Beschaffenheit gesetzt wird.

Wir schliessen diese Betrachtung des besonderen Falles

---

leicht hervorgehen, doch bedürfen wir desselben hier nicht in seiner Allgemeinheit.

mit einer bemerkenswerthen Folgerung ab. Hat man nämlich $2(\mu + 1)$ ganze Zahlen

$$\alpha_1\ \alpha_2 \cdots \alpha_{\mu+1}$$
$$\beta_1\ \beta_2 \cdots \beta_{\mu+1},$$

zwischen denen die Gleichung stattfindet

$$(30) \qquad \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_{\mu+1}\beta_{\mu+1} = 1,$$

so lässt sich eine unimodulare Determinante $\mu + 1^{\text{ten}}$ Grades angeben, in welcher $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$ die Elemente der ersten Zeile, und $\beta_1, \beta_2, \cdots \beta_{\mu+1}$ die ihnen adjungirten Elemente sind*). Denn, bestimmt man dem Vorigen entsprechend ein System vom Typus $\mu(\mu + 1)$, dessen Determinanten die Werthe $\beta_1, \beta_2, \cdots \beta_{\mu+1}$ haben, so bilden seine Zeilen zusammen mit den Elementen $\alpha_1, \alpha_2, \cdots \alpha_{\mu+1}$ eine solche Determinante D, da sie nach diesen Elementen entwickelt, gleich

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_{\mu+1}\beta_{\mu+1}$$

also wegen (30) gleich 1 ist. —

9. Wir wenden uns nunmehr zu den nicht-homogenen linearen Gleichungen

$$(31) \qquad A_\alpha = a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n = a_\alpha,$$
$$(\alpha = 1, 2, \cdots m < n)$$

zu denen wir durch die speciellen Gleichungen (16) und (17) schon geführt worden sind. Wir dürfen voraussetzen, dass diese Gleichungen unabhängig von einander sind. Mit ihnen kehren wir zu der Hauptaufgabe der Theorie der linearen Formen, zur Darstellung der Zahlen durch solche Formen oder durch ein System von solchen wieder zurück, denn, indem wir untersuchen, für welche a_α die Gleichungen in ganzen Zahlen auflösbar sind, gewinnen wir ein Bild von der Gesammtheit der Werthe, welche durch das System der m Linearformen darstellbar sind. Hier gilt nun vor allem folgender Satz**):

---

*) S. Journ. f. d. r. u. a. Math. 86 S. 150.

**) Dieser Satz findet sich zuerst bei J. Heger, Abh. der Wiener Akademie 14 II S. 111. S. auch Smith, On Systems etc. art. 111, sowie Frobenius, J. f. Math. 86 S. 171 Satz IV.

Zur Auflösbarkeit der Gleichungen (31) in ganzen Zahlen ist nothwendig und hinreichend, dass der grösste gemeinsame Theiler d aller Determinanten für das System a der Coefficienten der gleiche ist, wie für das durch die constanten Glieder *erweiterte* System $\mathfrak{a}$.

Diese Bedingung ist nothwendig; denn, wenn die Gleichungen (31) erfüllt sind, so ist jede Determinante von $\mathfrak{a}$, wenn sie die aus den constanten Gliedern bestehende Spalte nicht enthält, eine der Determinanten von a, andernfalls aber eine homogene lineare Funktion der letzteren, und somit ist jede Determinante von $\mathfrak{a}$ also auch ihr grösster gemeinsamer Theiler durch den grössten gemeinsamen Theiler d aller Determinanten von a theilbar, während andererseits in letzterem gewiss auch jener aufgehen muss: sie stimmen folglich nothwendig beide mit einander überein.

Die Bedingung ist aber auch hinreichend. Denn, bestimmt man die Einheitssysteme p, q nach der Formel

$$p \cdot a \cdot q = E, \tag{32}$$

wo E das Diagonalsystem

$$\begin{matrix} e_1 & 0 & \cdots & 0 & 0 & \cdots \\ 0 & e_2 & \cdots & 0 & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & e_m & 0 & \cdots \end{matrix}$$

bezeichnet, so führt man nach Cap. 2 nr. 2 die Gleichungen (31) auf m andere zurück von der Form

$$e_\alpha y_\alpha = a'_\alpha, \quad (\alpha = 1, 2, \cdots m) \tag{33}$$

welche jedenfalls eine Lösung in rationalen Zahlen y_α zulassen. Ferner aber erkennt man zufolge der Formel (6) jener nr., nämlich:

$$a'_\alpha = p_{\alpha 1} a_1 + p_{\alpha 2} a_2 + \cdots + p_{\alpha m} a_m \quad (\alpha = 1, 2, \cdots m)$$

sogleich die Richtigkeit folgender mit (32) analoger Beziehung:

$$p \cdot \mathfrak{a} \cdot q_0 = \mathfrak{E},$$

wenn unter q_0 das Einheitssystem

$$\begin{matrix} q_{11} & \cdots & q_{1n} & 0 \\ \cdot & \cdot & \cdot & \cdot \\ q_{n1} & \cdots & q_{nn} & 0 \\ 0 & \cdots & 0 & 1 \end{matrix}$$

und unter $\mathfrak{E}$ das durch die constanten Glieder a_α' erweiterte System E:

$$\begin{matrix} e_1 & 0 & \cdots & 0 & 0 & \cdots & a_1' \\ 0 & e_2 & \cdots & 0 & 0 & \cdots & a_2' \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & e_m & 0 & \cdots & a_m' \end{matrix}$$

verstanden wird. Mithin ist der grösste gemeinsame Theiler aller Determinanten des erweiterten Systems $\mathfrak{E}$ gleich demjenigen von $\mathfrak{a}$ oder a d. i. $d = e_1 e_2 \cdots e_m$. Nun sind aber die von 0 verschiedenen Determinanten von $\mathfrak{E}$ die folgenden Werthe:

$$d, \ \frac{d}{e_1} a_1', \ \frac{d}{e_2} a_2', \cdots \frac{d}{e_m} a_m';$$

demnach ist allgemein $\frac{a_\alpha'}{e_\alpha}$ eine ganze Zahl und die durch die Gleichungen (33) bestimmten Zahlen $y_1, y_2, \cdots y_m$ sind **ganzzahlig**. Führt man letztere in die Formeln (9) der nr. 2 des zweiten Capitels ein, so liefert diese:

$$x_\alpha = q_{\alpha 1} y_1 + q_{\alpha 2} y_2 + \cdots + q_{\alpha n} y_n$$
$$(\alpha = 1, 2, \cdots n)$$

eine ganzzahlige Auflösung der Gleichungen (31), welche ganzen Werthe auch den unbestimmt gebliebenen $y_{m+1}, y_{m+2}, \cdots y_n$ beigelegt werden, w. z. b. w. Und sie giebt zugleich ihre allgemeine Auflösung, wenn diesen Unbestimmten alle möglichen ganzen Zahlenwerthe ertheilt werden.

Man kann diese allgemeine Lösung auch folgendermassen finden. Bestimmt man nach nr. 5 zu den m Reihen von $m + \mu$ Elementen des Systems a noch μ Reihen

$$a_{m+\beta,1} \ a_{m+\beta,2} \cdots a_{m+\beta,m+\mu}$$
$$(\beta = 1, 2, \cdots \mu)$$

von der Beschaffenheit, dass die Determinante der $(m + \mu)^2$ Elemente gleich d wird, und bezeichnet mit

$$a_{m+1},\ a_{m+2},\ \cdots\ a_{m+\mu}$$

ganz willkürliche Zahlen, so kann man aus den $m + \mu$ Gleichungen

$$a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha, m+\mu} x_{m+\mu} = a_\alpha$$
$$(\alpha = 1, 2, \cdots m + \mu)$$

die Werthe x_i bestimmen und findet allgemein

$$(34) \qquad d \cdot x_i = - \left| a_{\alpha 1} \cdots a_{\alpha, i-1}\ a_\alpha\ a_{\alpha, i+1} \cdots a_{\alpha, m+\mu} \right|.$$

Wenn nun diese Determinante nach den Unterdeterminanten ihrer ersten m Zeilen entwickelt wird, so wird sie eine homogene lineare Funktion derjenigen Determinanten von $\mathfrak{a}$, welche die i^{te} Spalte nicht enthalten, der Divisor d lässt sich also gegen den grössten gemeinsamen Theiler der letzteren heben, und man erhält durch die Formel (34) eine Lösung der Gleichungen (31) in Gestalt einer ganzzahligen linearen Funktion von μ unbestimmten ganzen Zahlen

$$a_{m+1},\ a_{m+2},\ \cdots\ a_{m+\mu},$$

diese Formel muss daher der allgemeinen, vorher gefundenen Lösung der Gleichungen (31) gleichbedeutend sein.

10. Wir fügen an die Betrachtungen der vorigen nr. noch einige Bemerkungen an.

1) Aus der Formel (34) folgt unmittelbar, dass x_i theilbar ist durch $\frac{d^{(i)}}{d}$, wenn mit $d^{(i)}$ der grösste gemeinsame Theiler derjenigen Determinanten von $\mathfrak{a}$ bezeichnet wird, welche die i^{te} Spalte nicht enthalten. Betrachten wir nun, indem wir

$$a_{\alpha 0} = a_\alpha$$

setzen, neben dem Systeme (31) nicht homogener Gleichungen dasjenige homogener Gleichungen, welches folgt:

$$(35) \qquad a_{\alpha 0} x_0 + a_{\alpha 1} x_1 + \cdots + a_{\alpha n} x_n = 0.$$
$$(\alpha = 1, 2, \cdots m)$$

Unter der Voraussetzung, dass für die Systeme a und $\mathfrak{a}$ sämmtliche Determinanten denselben grössten gemeinsamen Theiler d haben oder dass $d^{(0)} = d$ sei, haben diese Gleichungen eine ganzzahlige Auflösung, bei welcher $x_0 = -1$, also, indem man die Vorzeichen bei derselben um-

kehrt, auch eine solche, bei welcher $x_0 = 1 = \frac{d^{(0)}}{d}$ ist. Wir wollen zeigen, dass sie auch eine solche ganzzahlige Auflösung haben, bei welcher $x_i = \frac{d^{(i)}}{d}$, oder auch eine solche, bei welcher $x_i = -\frac{d^{(i)}}{d}$ ist. In der That, das System der Gleichungen

$$(36) \qquad a_{\alpha 0}x_0 + \cdots + a_{\alpha, i-1}x_{i-1} + a_{\alpha, i+1}x_{i+1} + \cdots + a_{\alpha n}x_n = a_{\alpha i}\frac{d^{(i)}}{d}$$

ist in ganzen Zahlen auflösbar. Denn die Determinanten seines Coefficientensystems sind diejenigen Determinanten von $\mathfrak{a}$, welche die i^{te} Spalte nicht enthalten, und ihr grösster gemeinsamer Theiler ist folglich $d^{(i)}$. Dagegen sind die Determinanten des durch die constanten Glieder erweiterten Systems, wenn sie nicht mit den eben genannten identisch sind, solche Determinanten von $\mathfrak{a}$, welche die i^{te} Spalte enthalten, mal $\frac{d^{(i)}}{d}$, ihr grösster gemeinsamer Theiler ist also gleich $\delta^{(i)} \cdot \frac{d^{(i)}}{d}$, wenn $\delta^{(i)}$ der grösste gemeinsame Theiler der letzteren Determinanten und also d grösster gemeinsamer Theiler von $d^{(i)}$ und $\delta^{(i)}$ ist. Mithin ist für die Gleichungen (36) der grösste gemeinsame Theiler aller Determinanten des erweiterten Systems gleich demjenigen von $d^{(i)} = d \cdot \frac{d^{(i)}}{d}$ und $\delta^{(i)} \cdot \frac{d^{(i)}}{d}$ d. h., da $\delta^{(i)}$ theilbar sein muss durch d, gleich $d \cdot \frac{d^{(i)}}{d} = d^{(i)}$. Nach dem Satze der vorigen nr. ist demnach das System (36) von Gleichungen in ganzen Zahlen auflösbar.

Unter der gemachten Voraussetzung gestatten hiernach die Gleichungen (35) offenbar auch eine solche ganzzahlige Auflösung, bei der die Unbestimmte x_i irgend ein Vielfaches von $\frac{d^{(i)}}{d}$ ist*).

2) Wir können ferner bemerken, dass, wenn die Gleichungen (31) auflösbar sind, es auch die Gleichungen

*) St. Smith, On Systems etc. S. 311.

$$(37)\qquad a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n = b_\alpha$$
$$(\alpha = 1, 2, \cdots m)$$

sein werden, sobald $b_\alpha \equiv a_\alpha$ (mod. d) ist. Denn das System a ist für diese Gleichungen dasselbe wie für jene, und offenbar wird der grösste gemeinsame Theiler d aller Determinanten des erweiterten Systems $\mathfrak{a}$ unverändert bleiben, wenn die Elemente a_α dieses Systems durch irgend welche ihnen (mod. d) congruente Zahlen ersetzt werden. Die erforderliche Bedingung für die Auflösbarkeit der Gleichungen (37) ist also erfüllt. Man sieht hieraus, dass die Auflösbarkeit der Gleichungen (31) nur von den Resten abhängt, welche ihre rechten Seiten a_α (mod. d) lassen. Nun giebt es (mod. d) solcher Restsysteme a_α im Ganzen d^m; wir wollen untersuchen, für wieviel von ihnen die Gleichungen (31) auflösbar sind.

Da der Rang r von a gleich m ist, kann man nach nr. 7 des zweiten Capitels das Zahlensystem a allein durch Zusammensetzung mit Einheitssystemen zur Rechten auf die Gestalt (17a) dortselbst bringen d. h. die Gleichungen (31) durch eine Substitution anderer Variabeln y an Stelle der x durch diese:

$$(38)\qquad \begin{cases} a_1 = u_1 y_1 \\ a_2 = b_{21} y_1 + u_2 y_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_m = d_{m1} y_1 + d_{m2} y_2 + \cdots + d_{m,m-1} y_{m-1} + u_m y_m \end{cases}$$

ersetzen, in welchen $u_1 u_2 \cdots u_m = d$ sein muss; letztere Gleichungen sind mithin zugleich mit den Gleichungen (31) auflösbar oder nicht auflösbar. Die erste der Gleichungen (38) gestattet aber nur für $\frac{d}{u_1}$ Reste von a_1 (mod. d) ganzzahlige Auflösungen; für jeden von diesen liefert die zweite der Gleichungen nur $\frac{d}{u_2}$ verschiedene zulässige Reste von a_2 (mod. d) u. s. w., die letzte dann nur $\frac{d}{u_m}$ verschiedene Reste von a_m (mod. d). Somit giebt es nur

$$\frac{d}{u_1} \cdot \frac{d}{u_2} \cdots \frac{d}{u_m} = d^{m-1}$$

verschiedene Restsysteme a_α (mod. d), für welche

die Gleichungen (31) ganzzahlige Auflösungen gestatten*).

3) Wir beschliessen endlich dies Capitel mit der Frage nach der Aequivalenz von linearen Formen oder von Systemen solcher Formen. Wir definiren diese Aequivalenz in gewöhnlicher Weise: indem wir zwei Systeme von m (unabhängigen) Linearformen:

$$A_\alpha = a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n$$
$$(\alpha = 1, 2, \cdots m)$$

und

$$C_\alpha = c_{\alpha 1}z_1 + c_{\alpha 2}z_2 + \cdots + c_{\alpha n}z_n$$
$$(\alpha = 1, 2, \cdots m)$$

einander äquivalent nennen, sobald das eine in das andere durch eine unimodulare Substitution zwischen den Veränderlichen übergeht.

Nun kann man, wie soeben bemerkt, das System der Formen A_α mittels einer solchen unimodularen Substitution in das System der Linearformen (38) überführen, in welchem $u_1\, u_2 \cdots u_m = d$ ist und die übrigen Coefficienten die Bedingungen

$$0 \gtreqless b_{21} < u_1, \cdots 0 \gtreqless d_{m,1}, \cdots d_{m,m-1} < u_m$$

erfüllen. Wir wollen das letztere ein reducirtes Formensystem nennen; durch die reciproke Substitution verwandelt es sich wieder in das System A_α. Für das System der Linearformen C_α gilt dasselbe: auch ihm entspricht ein äquivalentes reducirtes Formensystem von derselben Gestalt. Betrachten wir nun neben dem System (38) ein zweites:

$$\begin{array}{l} u_1' y_1' \\ \beta_{21} y_1' + u_2' y_1' \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \delta_{m1} y_1' + \delta_{m2} y_2' + \cdots + u_m' y_m', \end{array}$$

wo $u_1' u_2' \cdots u_m' = d$ und

$$0 \gtreqless \beta_{21} < u_1', \cdots 0 \gtreqless \delta_{m,1}, \cdots \delta_{m,m-1} < u_m'$$

ist, und fragen, ob es mit (38) äquivalent sein kann. Da es

*) S. St. Smith a. a. O. S. 325, wo auch eine interessante Anwendung dieses Resultates gegeben wird.

alsdann aus letzterem Systeme durch eine unimodulare Substitution hervorgeht und dies nicht nur für die gesammten beiden Systeme, sondern auch allgemein für diejenigen beiden Theilsysteme gilt, welche aus den $\varkappa$ ersten der entsprechenden Formen bestehen, so muss der grösste gemeinsame Theiler aller Determinanten, die aus den ersten $\varkappa$ Gleichungen gebildet werden können, je derselbe sein, d. h.

$$u_1' u_2' \cdots u_\varkappa' = u_1 u_2 \cdots u_\varkappa$$

ebenso

$$u_1' u_2' \cdots u_{\varkappa-1}' = u_1 u_2 \cdots u_{\varkappa-1}$$

also allgemein $u_\varkappa' = u_\varkappa$. Aus der Gleichheit

$$u_1' y_1' = u_1 y_1$$

folgt dann $y_1' = y_1$; mithin aus der Gleichheit

$$\beta_{21} y_1 + u_2 y_2' = b_{21} y_1 + u_2 y_2$$

für jedes y_1 die Congruenz

$$b_{21} y_1 \equiv \beta_{21} y_1 \text{ d. h. } b_{21} \equiv \beta_{21} \pmod{u_2}$$

also nach den Ungleichheiten, welchen diese Zahlen unterworfen sind, $b_{21} = \beta_{21}$, mithin $y_2' = y_2$. Nun folgt aus der Gleichheit

$$\gamma_{31} y_1 + \gamma_{32} y_2 + u_3 y_3' = c_{31} y_1 + c_{32} y_2 + u_3 y_3,$$

welches auch y_1, y_2 sind, die Congruenz

$$\gamma_{31} y_1 + \gamma_{32} y_2 \equiv c_{31} y_1 + c_{32} y_2 \pmod{u_3}$$

d. h.

$$\gamma_{31} \equiv c_{31}, \ \gamma_{32} \equiv c_{32} \pmod{u_3}$$

oder vielmehr der beschränkenden Ungleichheiten wegen

$$\gamma_{31} = c_{31}, \ \gamma_{32} = c_{32} \text{ und folglich } y_3' = y_3,$$

u. s. w. Es ergiebt sich mithin als Bedingung für die Aequivalenz der beiden reducirten Systeme ihre völlige Identität.

Und hieraus folgt ohne Weiteres: Die zwei Systeme von Linearformen A_α und C_α sind dann und nur dann einander äquivalent, wenn sie ein- und dasselbe reducirte Formensystem haben. Die Coefficienten des reducirten Formensystems sind hiernach für die ganze Classe aller unter einander äquivalenten Systeme von Linearformen

unveränderlich dieselben und können deshalb als **die Invarianten des Systems der Linearformen** A_α betrachtet werden.

Dem Gefundenen zufolge giebt es ebensoviel nichtäquivalente Systeme von m unabhängigen Linearformen, als die Anzahl der reducirten Systeme beträgt; deren giebt es aber wegen der die Coefficienten beschränkenden Ungleichheiten für jede Zerlegung

$$d = u_1 u_2 \cdots u_m \tag{39}$$

der Zahl d in m Faktoren

$$u_2 \cdot u_3^2 \cdots u_m^{m-1} = \frac{1}{d} \cdot u_1 u_2^2 \cdots u_m^m,$$

im Ganzen also

$$\frac{1}{d} \cdot \sum u_1 u_2^2 \cdots u_m^m, \tag{40}$$

wenn die Summation auf alle Zerlegungen (39) sich bezieht. Denken wir uns d in Primzahlpotenzen zerlegt:

$$d = \prod_p p^\delta, \tag{41}$$

setzen dann

$$u_\varkappa = \prod_p p^{\delta_\varkappa},$$

so sind die Exponenten $\delta_\varkappa$ wegen (39) durch die Bedingung

$$\delta_1 + \delta_2 + \cdots + \delta_m = \delta \tag{42}$$

mit einander verbunden, und man erhält statt des Ausdrucks (40) den folgenden:

$$\frac{1}{d} \sum \left(\prod_p p^{\delta_1 + 2\delta_2 + \cdots + m\delta_m} \right),$$

wo die Summation auch mit der Multiplikation vertauscht und

$$\frac{1}{d} \prod_p \left(\sum p^{\delta_1 + 2\delta_2 + \cdots + m\delta_m} \right) \tag{43}$$

geschrieben werden darf. Hier sind die Glieder der Summe, die auf alle Lösungen der Gleichung (42) auszudehnen ist, identisch mit den Gliedern der Entwicklung von

$$(p + p^2 + \cdots + p^m)^\delta,$$

wenn diese nur einfach, ohne ihren Polynomialcoefficienten,

genommen werden. Insbesondere sind sie für $\delta = 1$ die Glieder der Summe

$$p + p^2 + \cdots + p^m$$

selbst, und somit wird der Ausdruck (40) oder (43) d. i. die Anzahl der reducirten *Formensysteme* in dem einfachen Falle, wo d aus lauter verschiedenen Primfaktoren besteht, gleich

$$\prod_p \frac{p^m - 1}{p - 1} \text{*)}.$$

Viertes Capitel.

Die linearen Congruenzen.

1. Von den linearen Gleichungen wenden wir uns jetzt noch zu den linearen Congruenzen, deren wir ein System von m Congruenzen

$$(1) \qquad A_\alpha \equiv a_\alpha \pmod{\varkappa}$$
$$(\alpha = 1, 2, \cdots m)$$

betrachten wollen. Offenbar sind diese m Congruenzen durchaus gleichbedeutend mit den m Gleichungen

$$(2) \qquad A_\alpha + \varkappa z_\alpha = a_\alpha,$$
$$(\alpha = 1, 2, \cdots m)$$

auf deren Betrachtung wir mithin die Untersuchung der ersteren zurückführen können.

Seien zuerst die Congruenzen homogen also $a_\alpha = 0$; es handelt sich dann um die Auflösung der m homogenen Gleichungen

$$(3) \qquad A_\alpha + \varkappa z_\alpha = 0.$$
$$(\alpha = 1, 2, \cdots m)$$

Wenn mit p, q wieder dieselben Einheitssysteme bezeichnet werden, wie in Cap. 2, nr. 2, so lassen sich die Gleichungen durch passende Combination auf die Gestalt

---

*) S. Abschnitt 1, Cap. 7 nr. 1.

[illegible]

$$[illegible] = [illegible]$$

$$\cdots y_\alpha - x z_\alpha' = [illegible]$$

[illegible]

$$y_\alpha = \frac{x}{s_\alpha} \cdot \zeta_\alpha, \quad z_\alpha' = -\frac{e_\alpha}{s_\alpha} \cdot \zeta_\alpha,$$

[illegible] ζ_α [illegible] ganze Zahl bedeutet. Man findet [illegible] Lösung der Gleichungen (7) die folgende:

$$(8) \quad \begin{cases} y_1 = \frac{x}{s_1} \zeta_1, \; y_2 = \frac{x}{s_2} \zeta_2 \cdots y_r = \frac{x}{s_r} \zeta_r, \\ y_{r+1} \cdots y_n \text{ beliebig}. \\ z_1' = -\frac{e_1}{s_1} \zeta_1, \; z_2' = -\frac{e_2}{s_2} \zeta_2 \cdots z_r' = -\frac{e_r}{s_r} \zeta_r, \\ z_{r+1}', \cdots z_m' \text{ gleich Null.} \end{cases}$$

Hieraus aber findet sich die allgemeinste Lösung der Gleichungen (3), wenn einerseits die Werthe z_α' in (4) eingesetzt und dann aus diesen Gleichungen die z_α bestimmt werden,

andererseits durch Substitution der gefundenen Werthe der y_α in die Gleichungen (5), wodurch man findet:

$$(9)\quad x_\alpha = q_{\alpha 1}\cdot\frac{\varkappa}{s_1}\zeta_1 + \cdots + q_{\alpha r}\cdot\frac{\varkappa}{s_r}\zeta_r + q_{\alpha, r+1}\zeta_{r+1} + \cdots + q_{\alpha n}\zeta_n,$$
$$(\alpha = 1, 2, \cdots n)$$

wenn die ζ_i ganz beliebige ganze Zahlen bezeichnen. Diese Werthe x_α sind dann zugleich die allgemeinste Lösung der Congruenzen

$$(10)\qquad A_\alpha \equiv 0 \pmod{\varkappa}.$$
$$(\alpha = 1, 2, \cdots m)$$

Handelt es sich nun darum, aus allen diesen die unter einander incongruenten Lösungen auszuscheiden resp. ihre Anzahl zu bestimmen, so kann man bemerken, dass, da der Modulus der Substitution (5) die Einheit ist, offenbar nicht nur congruenten Systemen der y congruente Systeme der x entsprechen, sondern auch umgekehrt, und folglich muss die Anzahl der (mod. $\varkappa$) incongruenten Systeme (9) der Zahlen x_α gleich derjenigen der incongruenten Systeme (8) der Zahlen y_α sein. Die letztere ist aber ersichtlich

$$s_1 s_2 \cdots s_r \cdot \varkappa^{n-r};$$

kommt man also überein, $s_h = \varkappa$ zu setzen, so oft $h > r$ ist, so findet sich die Anzahl $|A, \varkappa|$ der *incongruenten* Lösungen oder der *Wurzeln* der Congruenzen (10) durch die Formel:

$$(11)\qquad |A, \varkappa| = s_1 s_2 \cdots s_n.$$

Da e_h durch e_{h-1} theilbar ist, so geht auch der grösste gemeinsame Theiler s_h von e_h und $\varkappa$ durch den grössten gemeinsamen Theiler s_{h-1} von e_{h-1} und $\varkappa$ auf; folglich ist $\frac{\varkappa}{s_{h-1}}$ theilbar durch $\frac{\varkappa}{s_h}$. Der Formel (9) zufolge ist deshalb, so oft der Rang r des Systems a gleich n ist, jede der Zahlen x_α theilbar durch $\frac{\varkappa}{s_n}$, und folglich können alsdann die Elemente $x_1, x_2, \cdots x_n$ einer Lösung der Congruenzen (10) nur unter der Bedingung, dass $s_n = \varkappa$ d. h. e_n durch $\varkappa$ theilbar ist, Zahlen ohne einen gemeinsamen Theiler sein. Da ferner, falls $r < n$ ist, $e_n = 0$ also gleichfalls theilbar ist durch $\varkappa$, dürfen

wir sagen: die Congruenzen (10) können nur dann eine Lösung in Zahlen ohne gemeinsamen Theiler haben, wenn e_n theilbar ist durch $\varkappa$. Umgekehrt aber, wenn e_n durch $\varkappa$ aufgeht also $s_n = \varkappa$ ist, so ist entweder $r = n$ also

$$x_\alpha = q_{\alpha 1} \cdot \frac{\varkappa}{s_1} \zeta_1 + \cdots + q_{\alpha n} \cdot \frac{\varkappa}{s_n} \zeta_n, \quad (\alpha = 1, 2, \cdots n)$$

oder r ist $< n$ und es gilt die Formel (9); in beiden Fällen findet man, indem man $\zeta_n = 1$, die übrigen ζ gleich Null wählt, die Lösung

$$x_1 = q_{1n}, \; x_2 = q_{2n} \cdots x_n = q_{nn},$$

welches eine Lösung in Zahlen ohne gemeinsamen Theiler ist, da die Determinante des Systems q, von welchem diese Zahlen eine Spalte bilden, gleich 1 ist. — Beide Ergebnisse zusammenfassend gewinnt man folgenden Satz:

Damit mehrere homogene lineare Congruenzen zwischen n Unbekannten eine Lösung in ganzen Zahlen ohne gemeinsamen Theiler haben, ist nothwendig und hinreichend, dass der Modul der Congruenzen im n^{ten} Elementartheiler des Coefficientensystems aufgehe*).

Jeder Lösung der Congruenzen (10) in Zahlen $x_1, x_2, \cdots x_n$ ohne gemeinsamen Theiler entspricht ein System rationaler Werthe

$$\xi_1 = \frac{x_1}{\varkappa}, \; \xi_2 = \frac{x_2}{\varkappa}, \cdots \xi_n = \frac{x_n}{\varkappa}$$

mit dem Generalnenner $\varkappa$, für welches die m Linearformen

$$(12) \qquad a_{\alpha 1}\xi_1 + a_{\alpha 2}\xi_2 + \cdots + a_{\alpha n}\xi_n \quad (\alpha = 1, 2, \cdots m)$$

ganzzahlig werden, und umgekehrt. Demnach lässt sich der vorige Satz auch in dieser andern Fassung aussprechen:

Damit die Linearformen (12) für rationale Werthe der Variabeln ganzzahlig werden können, ist nothwendig und hinreichend, dass der n^{te} Elementartheiler

*) S. Frobenius, Theorie der linearen Formen mit ganzen Coefficienten, J. für Math. 86 S. 192.

des Coefficientensystems durch ihren Generalnenner theilbar sei*).

2. Indem man in den m Ausdrücken

$$A_\alpha = a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + \cdots + a_{\alpha n}x_n$$
$$(\alpha = 1, 2, \cdots m)$$

den Unbestimmten $x_1, x_2, \cdots x_n$ irgend ein System von Resten

$$r_1', r_2', \cdots r_n' \pmod{\varkappa}$$

beilegt, erhält man ein System zugehöriger Werthe

$$A_1', A_2', \cdots A_m',$$

und wenn dies auf alle mögliche Weise geschieht, $\varkappa^n$ solcher Systeme. Entspricht ein zweites derselben:

$$A_1'', A_2'', \cdots A_m''$$

dem System $r_1'', r_2'', \cdots r_n''$ von Resten, so wird es dem ersteren (mod. $\varkappa$) congruent sein oder nicht, je nachdem die Zahlen

$$r_1'' - r_1', r_2'' - r_2', \cdots r_n'' - r_n'$$

eine Wurzel der Congruenzen (10) darstellen oder nicht. Mithin werden je $|A, \varkappa|$ Systeme von Resten der Unbestimmten congruente Systeme A_α ergeben und die Anzahl $(A, \varkappa)$ nichtcongruenter Werthsysteme, welche die m Linearformen A_α (mod. $\varkappa$) lassen können, wird durch die Gleichung

$$(A, \varkappa) \cdot |A, \varkappa| = \varkappa^n \tag{13}$$

bestimmt sein. Mit Rücksicht auf (11) findet sich also die Formel:

$$(A, \varkappa) = \frac{\varkappa^n}{s_1 s_2 \cdots s_n} = \prod_{h=1}^{n} \left(\frac{\varkappa}{s_h}\right) = \prod_{h=1}^{r} \left(\frac{\varkappa}{s_h}\right). \tag{14}$$

Diesem Ausdrucke für $(A, \varkappa)$ lassen sich ein paar andere Bestimmungsweisen an die Seite stellen, die oft nützlich verwendet werden können. Wir zeigen zu diesem Zwecke, dass $s_1 s_2 \cdots s_r$ der grösste gemeinsame Theiler der Zahlen

$$\varkappa^r, \varkappa^{r-1}d_1, \varkappa^{r-2}d_2, \cdots \varkappa d_{r-1}, d_r \tag{15}$$

oder der Zahlen

---

*) Vgl. hierzu Hensel, zur Theorie der linearen Formen, J. für Math. 107 S. 241.

$$\varkappa^r, \varkappa^{r-1}e_1, \varkappa^{r-2}e_1e_2, \cdots \varkappa \cdot e_1e_2 \cdots e_{r-1}, e_1e_2 \cdots e_r$$

ist. In der That: die beiden ersten von ihnen haben den grössten gemeinsamen Theiler $\varkappa^{r-1}s_1$, folglich sie alle denselben grössten gemeinsamen Theiler wie die folgenden:

$$(16) \qquad \varkappa^{r-1}s_1, \varkappa^{r-2}e_1e_2, \varkappa^{r-3}e_1e_2e_3, \cdots e_1e_2 \cdots e_r.$$

Von den letzteren haben die beiden ersten zum grössten gemeinsamen Theiler $\varkappa^{r-2}$ mal denjenigen von

$$\varkappa s_1 = \frac{\varkappa}{s_2} \cdot s_1 s_2 \text{ und } e_1 e_2 = \frac{e_1}{s_1} \frac{e_2}{s_2} \cdot s_1 s_2;$$

hier ist aber $\frac{\varkappa}{s_2}$ prim gegen $\frac{e_2}{s_2}$ und als Theiler von $\frac{\varkappa}{s_1}$ auch gegen $\frac{e_1}{s_1}$, mithin haben die genannten beiden Zahlen den grössten gemeinsamen Theiler $\varkappa^{r-2}s_1s_2$, und die Zahlen (16) genau denselben, wie die folgenden:

$$\varkappa^{r-2}s_1s_2, \varkappa^{r-3}e_1e_2e_3, \cdots, e_1e_2 \cdots e_r$$

u. s. f., sodass sich schliesslich $s_1s_2 \cdots s_r$ als grösster gemeinsamer Theiler a l l e r Zahlen (15) herausstellt.

Schreibt man demnach die Zahlen

$$(17) \qquad \varkappa^n, \varkappa^{n-1}d_1, \varkappa^{n-2}d_2, \cdots \varkappa d_{n-1}, d_n,$$

von denen, wenn $r < n$ ist, die letzten $n - r$ gleich Null sind, so werden diese

$$s_1 s_2 \cdots s_r \cdot \varkappa^{n-r} = s_1 s_2 \cdots s_n$$

zum grössten gemeinsamen Theiler haben. So geht der Satz hervor:

Die mit $|A, \varkappa|$ bezeichnete Anzahl ist der grösste gemeinsame Theiler aller Zahlen (17), und man findet die Zahl $(A, \varkappa)$, wenn man $\varkappa^n$ durch den letzteren dividirt. Wenn man aber die Brüche

$$(18) \qquad \frac{d_1}{\varkappa}, \frac{d_2}{\varkappa^2}, \cdots \frac{d_n}{\varkappa^n}$$

oder

$$\frac{\varkappa^{n-1}d_1}{\varkappa^n}, \frac{\varkappa^{n-2}d_2}{\varkappa^n}, \cdots \frac{d_n}{\varkappa^n}$$

auf ihren Generalnenner bringt, wird der letztere offenbar in genau derselben Weise erhalten. U n d s o m i t k a n n m a n

$(A, \varkappa)$ auch als den Generalnenner der Brüche (18) definiren.

Nach (11) erhält die Zahl $|A, \varkappa|$ dann und nur dann den Werth 1, wenn $\varkappa$ prim ist gegen d_n. Man schliesst folglich den Satz: Die Congruenzen (10) haben dann und nur dann die einzige Lösung $x_\alpha \equiv 0 \pmod{\varkappa}$, wenn $r = n$ und $\varkappa$ zum grössten gemeinsamen Theiler aller Determinanten von a prim ist*).

Denken wir uns nunmehr neben den m Linearformen

$$(19) \qquad a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha n} x_n \quad (\alpha = 1, 2, \cdots m)$$

mit n Unbestimmten dasjenige System von n Linearformen

$$(20) \qquad a_{1\beta} y_1 + a_{2\beta} y_2 + \cdots + a_{m\beta} y_m \quad (\beta = 1, 2, \cdots n)$$

mit m Unbestimmten, dessen Zahlensystem a' das zu a conjugirte System ist.

Da, wie bereits am Ende von nr. 4 des zweiten Capitels bemerkt worden ist, die Elementartheiler von a' identisch sind mit denjenigen von a, so müssen für a' auch die grössten gemeinsamen Theiler von $\varkappa$ und den Elementartheilern dieselben Zahlen $s_1, s_2, \cdots s_n$ sein, wie für a, und somit ergiebt sich aus (14) ohne weiteres die Gleichheit:

$$(21) \qquad (A', \varkappa) = (A, \varkappa)$$

oder der Satz**): Die Anzahl der (mod. $\varkappa$) incongruenten, durch die m Formen (19) darstellbaren Werthsysteme ist ebenso gross, wie die Anzahl der (mod. $\varkappa$) incongruenten Werthsysteme, welche durch die n conjugirten Formen (20) darstellbar sind.

Heisst aber $|A', \varkappa|$ die Anzahl incongruenter Lösungen des zu (10) conjugirten Systems von Congruenzen:

$$a_{1\beta} y_1 + a_{2\beta} y_2 + \cdots + a_{m\beta} y_m \equiv 0 \pmod{\varkappa} \quad (\beta = 1, 2, \cdots n)$$

mit den m Unbestimmten $y_1, y_2, \cdots y_m$, so ist der Formel (13) entsprechend

*) Journ. f. d. r. u. a. Math. 86 S. 193.

**) S. Frobenius Th. d. lin. Formen, J. f. Math. 86 S. 192.

$$(A', \varkappa) \cdot | A', \varkappa | = \varkappa^m,$$

mithin wegen (21)

$$| A, \varkappa | : | A', \varkappa | = \varkappa^n : \varkappa^m;$$

nur also, wenn $m = n$ ist, gilt die Gleichheit

$$| A', \varkappa | = | A, \varkappa |.$$

3. Wir wollen nun annehmen, dass die Congruenzen (10) **unabhängige** Congruenzen also $r = m \overline{\gtrless} n$ sei. Ihre allgemeine Lösung wird dann durch die Formel

$$(22) \quad x_\alpha = q_{\alpha 1} \frac{\varkappa}{s_1} \zeta_1 + \cdots + q_{\alpha, m} \frac{\varkappa}{s_m} \zeta_m + q_{\alpha, m+1} \zeta_{m+1} + \cdots + q_{\alpha n} \zeta_n$$
$$(\alpha = 1, 2, \cdots n)$$

geliefert, indem man darin für $\zeta_1, \zeta_2, \cdots \zeta_n$ alle ganzen Zahlen setzt; auch ist jedes so gelieferte System von Werthen x_1, $x_2, \cdots x_n$ eine jener Lösungen und man erhält jede von ihnen auch nur einmal. Insbesondere sind die n Systeme

$$(23) \quad \begin{cases} q_{11} \frac{\varkappa}{s_1} & q_{21} \frac{\varkappa}{s_1} & \cdots & q_{n1} \frac{\varkappa}{s_1} \\ \cdot & \cdot & \cdot & \cdot \\ q_{1m} \frac{\varkappa}{s_m} & q_{2m} \frac{\varkappa}{s_m} & \cdots & q_{nm} \frac{\varkappa}{s_m} \\ q_{1, m+1} & q_{2, m+1} & \cdots & q_{n, m+1} \\ \cdot & \cdot & \cdot & \cdot \\ q_{1n} & q_{2n} & \cdots & q_{nn} \end{cases}$$

auch n Lösungen der Congruenzen (10), aus denen, wie die Formel (22) zeigt, alle übrigen Lösungen sich linear zusammensetzen lassen. Da q ein Einheitssystem ist, findet sich als Werth der Determinante des vorstehenden Systems offenbar

$$\frac{\varkappa^m}{s_1 s_2 \cdots s_m} = \frac{\varkappa^n}{s_1 s_2 \cdots s_n} = (A, \varkappa).$$

Es giebt mithin für die von einander unabhängigen Congruenzen

$$A_\alpha \equiv 0 \pmod{\varkappa}$$
$$(\alpha = 1, 2, \cdots m)$$

mit n Unbestimmten n Lösungen, deren Determinante

gleich $(A, \varkappa)$ ist und aus welchen alle übrigen linear zusammensetzbar sind*).

Diese Lösungen könnte man füglich, wie bei den Gleichungen, ein System fundamentaler Lösungen der Congruenzen nennen. Indessen wollen wir diesen Ausdruck hier anders gebrauchen. Da es nämlich bei Congruenzen wesentlich nur auf incongruente Lösungen oder Wurzeln ankommt, so wollen wir λ Lösungen

$$b_{\alpha 1}\; b_{\alpha 2} \cdots b_{\alpha n} \quad (\alpha = 1, 2, \cdots \lambda) \tag{24}$$

der Congruenzen (10) dann ein System von Fundamentalauflösungen nennen, wenn alle incongruenten Lösungen $x_1, x_2, \cdots x_n$ durch die Formel

$$x_\alpha \equiv b_{1\alpha} z_1 + b_{2\alpha} z_2 + \cdots + b_{\lambda\alpha} z_\lambda \pmod{\varkappa} \quad (\alpha = 1, 2, \cdots n) \tag{25}$$

gegeben werden, indem man für die Unbestimmten $z_1, z_2, \cdots z_\lambda$ alle Reste (mod. $\varkappa$) einsetzt. Es ist leicht, eine Bedingung abzuleiten, welche dafür, dass die Lösungen (24) ein solches Fundamentalsystem bilden, nothwendig und hinreichend ist. Da nämlich die Ausdrücke (25) stets den Congruenzen (10) genügen, wenn dies die Zahlen (24) thun, werden letztere offenbar dann und nur dann ein Fundamentalsystem bilden, wenn jene Ausdrücke genau so viel (mod. $\varkappa$) incongruente Systeme x_α darstellen können, als die Congruenzen (10) Wurzeln haben. Bezeichnet man also mit $(B, \varkappa)$ die Anzahl der (mod. $\varkappa$) incongruenten Werthsysteme, welche die n Formen

$$b_{1\alpha} z_1 + b_{2\alpha} z_2 + \cdots + b_{\lambda\alpha} z_\lambda \quad (\alpha = 1, 2, \cdots n)$$

mit λ Unbestimmten oder, was dasselbe sagt, welche die conjugirten λ Formen

$$b_{\alpha 1} y_1 + b_{\alpha 2} y_2 + \cdots + b_{\alpha n} y_n \quad (\alpha = 1, 2, \cdots \lambda)$$

mit n Unbestimmten darstellen können, so ist die nothwendige und hinreichende Bedingung dafür, dass

*) Frobenius a. a. O. S. 182.

die Lösungen (24) ein Fundamentalsystem der Congruenzen (10) bilden, die Gleichheit:

(26) $$|A, \varkappa| = (B, \varkappa).$$

Da der Voraussetzung nach allgemein

$$a_{\alpha 1} b_{\beta 1} + a_{\alpha 2} b_{\beta 2} + \cdots + a_{\alpha n} b_{\beta n} \equiv 0 \pmod{\varkappa}$$
$$(\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots \lambda)$$

ist, so leuchtet ein, dass die m Werthreihen

(27) $$a_{\alpha 1}\ a_{\alpha 2}\ \cdots\ a_{\alpha n}$$
$$(\alpha = 1, 2, \cdots m)$$

des Systems a ebenso viel Lösungen der λ Congruenzen

(28) $$b_{\beta 1} y_1 + b_{\beta 2} y_2 + \cdots + b_{\beta n} y_n \equiv 0 \pmod{\varkappa}$$
$$(\beta = 1, 2, \cdots \lambda)$$

sind. Nennt man $|B, \varkappa|$ die Anzahl incongruenter Lösungen der letzteren, so besteht die mit (13) analoge Beziehung

$$|B, \varkappa| \cdot (B, \varkappa) = \varkappa^n.$$

Ist folglich die Gleichung (26) erfüllt d. h. das System (24) von Lösungen der Congruenzen (10) ein fundamentales, so folgt die Gleichung

$$|B, \varkappa| = (A, \varkappa)$$

und daher werden auch die Lösungen (27) der Congruenzen (28) ein fundamentales System von Lösungen der letzteren sein. Dieser eigenthümlichen Reciprocität zwischen den beiden Congruenzensystemen (10) und (27) halber nennt man sie einander adjungirt.

Nimmt man an, der grösste gemeinsame Theiler aller Determinanten h^{ten} Grades des Systems a sei prim gegen den Modulus $\varkappa$, dagegen derjenige aller Determinanten $h + 1^{\text{ten}}$ Grades sei es nicht, so ist $s_{h+1} > 1$, aber s_h und folglich auch $s_{h-1}, s_{h-2}, \cdots s_1$ sind gleich 1. Dann verwandeln sich aber die Gleichungen (9) in folgende Congruenzen:

$$x_\alpha \equiv q_{\alpha, h+1} \cdot \frac{\varkappa}{s_{h+1}} \cdot \zeta_{h+1} + \cdots + q_{\alpha m} \cdot \frac{\varkappa}{s_m} \cdot \zeta_m$$
$$+ q_{\alpha, m+1} \zeta_{m+1} + \cdots + q_{\alpha n} \zeta_n$$
$$(\alpha = 1, 2, \cdots n)$$

(mod. $\varkappa$), welche lehren, dass das System

$$(29)\quad \begin{cases} q_{1,h+1}\frac{\varkappa}{s_{h+1}} & q_{2,h+1}\frac{\varkappa}{s_{h+1}} & \cdots q_{n,h+1}\frac{\varkappa}{s_{h+1}} \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\ q_{1m}\frac{\varkappa}{s_m} & q_{2m}\frac{\varkappa}{s_m} & \cdots q_{nm}\frac{\varkappa}{s_m} \\ q_{1,m+1} & q_{2,m+1} & \cdots q_{n,m+1} \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\ q_{1n} & q_{2n} & \cdots q_{nn} \end{cases}$$

ein System von $n - h$ fundamentalen Lösungen der Congruenzen (10) ist. Es giebt aber kein System von Fundamentalauflösungen, welche aus einer geringeren Anzahl Lösungen bestände. In der That, wäre, wenn $\lambda = n - h - \mu$ gedacht wird, das System (24) ein solches, so müssten, wenn

$$x_{1\beta}\ x_{2\beta} \cdots x_{n\beta}$$

die β^{te} Reihe von (29) bezeichnen, die Congruenzen statthaben:

$$x_{\alpha\beta} \equiv b_{1\alpha}z_{1\beta} + b_{2\alpha}z_{2\beta} + \cdots + b_{\lambda\alpha}z_{\lambda\beta} \pmod{\varkappa}$$
$$(\alpha = 1, 2, \cdots n;\ \beta = 1, 2, \cdots n - h);$$

und man bemerke, dass

$$b_{1\alpha}z_{1\beta} + b_{2\alpha}z_{2\beta} + \cdots + b_{\lambda\alpha}z_{\lambda\beta} = \frac{\varkappa}{s_{h+\beta}}\cdot\zeta_{\alpha\beta}$$

wo $\zeta_{\alpha\beta}$ ganzzahlig ist, gesetzt werden darf. Demnach lässt sich das System (29) auf jede der beiden nachstehenden Arten schreiben:

$$(30)\quad \begin{cases} b_{11}z_{11} + \cdots + b_{\lambda 1}z_{\lambda 1} + \varkappa\xi_{11}, \\ b_{12}z_{11} + \cdots + b_{\lambda 2}z_{\lambda 1} + \varkappa\xi_{21}, \cdots; \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ ; \\ b_{11}z_{1,n-h} + \cdots + b_{\lambda 1}z_{\lambda,n-h} + \varkappa\xi_{1,n-h}, \\ b_{12}z_{1,n-h} + \cdots + b_{\lambda 2}z_{\lambda,n-h} + \varkappa\xi_{2,n-h}, \cdots, \end{cases}$$

oder:

$$(31)\quad \begin{cases} \frac{\varkappa}{s_{h+1}}\zeta_{11} + \varkappa\xi_{11}, \quad \frac{\varkappa}{s_{h+1}}\zeta_{21} + \varkappa\xi_{21}, \cdots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \frac{\varkappa}{s_n}\zeta_{1,n-h} + \varkappa\xi_{1,n-h}, \quad \frac{\varkappa}{s_n}\zeta_{2,n-h} + \varkappa\xi_{2,n-h}, \cdots, \end{cases}$$

worin auch die ξ ganze Zahlen bedeuten. Nimmt man nun irgend eine Determinante $n - h^{\text{ten}}$ Grades des Systems (29)

und entwickelt man sie den Formen (30) oder (31) zufolge nach Potenzen von $\varkappa$, so zeigt die erste dieser Formen, dass die Glieder mit geringeren Potenzen als $\varkappa^\mu$ identisch verschwinden; der Form (31) zufolge aber ist das Glied der entwickelten Determinante, welches $\varkappa^\mu$ enthält, gleich $\varkappa^\mu$ mal einem Aggregate von Determinanten λ^{ten} Grades des Systems

$$\begin{array}{cccc} \frac{\varkappa}{s_{h+1}}\zeta_{11}, & \frac{\varkappa}{s_{h+1}}\zeta_{21}, & \cdots & \frac{\varkappa}{s_{h+1}}\zeta_{n1}, \\ \cdot & \cdot & \cdot & \cdot \\ \frac{\varkappa}{s_n}\zeta_{1,n-h}, & \frac{\varkappa}{s_n}\zeta_{2,n-h}, & \cdots & \frac{\varkappa}{s_n}\zeta_{n,n-h}, \end{array}$$

ein Aggregat, welches gewiss den Faktor

$$\frac{\varkappa^\lambda}{s_{h+\mu+1}\,s_{h+\mu+2}\cdots s_n}$$

enthält, und ist also theilbar durch

$$\frac{\varkappa^{n-h}}{s_{h+\mu+1}\,s_{h+\mu+2}\cdots s_n}.$$

Ebenso ist das Glied der entwickelten Determinante, welches $\varkappa^{\mu+1}$ enthält, theilbar durch $\frac{\varkappa^{n-h}}{s_{h+\mu+2}\cdots s_n}$ u. s. w., das letzte Glied theilbar durch $\varkappa^{n-h}$. Die ganze Determinante $n-h^{\text{ten}}$ Grades des Systems (29), die wir betrachten, wird mithin gewiss durch den grössten gemeinsamen Theiler der eben bezeichneten Zahlen d. i. durch

$$\frac{\varkappa^{n-h}}{s_{h+\mu+1}\,s_{h+\mu+2}\cdots s_n}$$

aufgehen, und da diese Determinante irgend eine der Determinanten $n-h^{\text{ten}}$ Grades jenes Systems ist, muss auch der letzteren grösster gemeinsamer Theiler, welcher, da q ein Einheitssystem ist, den Werth

$$\frac{\varkappa^{n-h}}{s_{h+1}\,s_{h+2}\cdots s_n}$$

hat, durch den vorigen Werth theilbar sein und folglich der Quotient

$$\frac{s_{h+\mu+1}\,s_{h+\mu+2}\cdots s_n}{s_{h+1}\,s_{h+2}\cdots s_n}$$

eine ganze Zahl. Dies ist aber nicht der Fall, wenn $\mu > 0$ d. h. $\lambda < n - h$ ist. —

Auf solche Weise ist folgender Satz gewonnen worden*): Wenn im Systeme a der grösste gemeinsame Theiler aller Determinanten h^{ten} Grades prim gegen $\varkappa$, derjenige aller Determinanten $h+1^{\text{ten}}$ Grades aber nicht prim gegen $\varkappa$ ist, so giebt es für die Congruenzen (10) ein System von $n-h$ Fundamentalauflösungen, aber kein solches System, das aus weniger als $n-h$ Lösungen bestände.

4. Der Fall nicht homogener Congruenzen

$$A_\alpha \equiv a_\alpha \pmod{\varkappa} \quad (\alpha = 1, 2, \cdots m) \tag{32}$$

bietet nach den im Vorigen entwickelten Resultaten keine Schwierigkeit mehr. Wir dürfen die Congruenzen als unabhängige voraussetzen.

Ist dann zuerst $m \overline{\overline{<}} n$, so wird $r = m$ sein. Da die Congruenzen den Gleichungen

$$A_\alpha + \varkappa z_\alpha = a_\alpha \quad (\alpha = 1, 2, \cdots m) \tag{33}$$

vollkommen gleichbedeutend sind, erhalten wir zuvörderst die nothwendige und hinreichende Bedingung für ihre Auflösbarkeit durch Anwendung des in nr. 9 des dritten Capitels gegebenen Kriteriums: der grösste gemeinsame Theiler aller Determinanten muss derselbe sein für die beiden Systeme:

$$\begin{matrix} a_{11} & \cdots & a_{1n} & \varkappa & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & \cdots & a_{mn} & 0 & 0 & \cdots & \varkappa \end{matrix} \quad \text{und} \quad \begin{matrix} a_1 & a_{11} & \cdots & a_{1n} & \varkappa & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_m & a_{m1} & \cdots & a_{mn} & 0 & 0 & \cdots & \varkappa. \end{matrix}$$

Nun sind die Determinanten des ersten Systems 1) die sämmtlichen Determinanten m^{ten} Grades von a, 2) die mit $\varkappa$ multiplicirten Determinanten $m-1^{\text{ten}}$ Grades, 3) die mit $\varkappa^2$ multiplicirten Determinanten $m-2^{\text{ten}}$ Grades von a, u. s. w., endlich $\varkappa^m$. Ihr grösster gemeinsamer Theiler ist also mit demjenigen der Zahlen

$$\varkappa^m, \ \varkappa^{m-1} \cdot d_1, \ \varkappa^{m-2} \cdot d_2, \ \cdots \varkappa \cdot d_{m-1}, \ d_m$$

*) S. Frobenius J. f. Math. 88 S. 109.

identisch, welcher sich, wie in nr. 2, gleich $s_1 s_2 \cdots s_m$ ergiebt. Bezeichnet man für das erweiterte System die grössten gemeinsamen Theiler der Determinanten verschiedener Grade mit $\delta_1, \delta_2, \cdots \delta_n$, mit $\varepsilon_1, \varepsilon_2, \cdots \varepsilon_n$ die Elementartheiler und mit $\sigma_1, \sigma_2, \cdots \sigma_n$ ihre grössten gemeinsamen Theiler mit $\varkappa$, so findet sich der grösste gemeinsame Theiler aller Determinanten des obigen zweiten Systems durch dieselbe Betrachtung gleich $\sigma_1 \sigma_2 \cdots \sigma_m$. Und somit ist die nothwendige und hinreichende Bedingung für die Auflösbarkeit der Congruenzen (32) im Falle $m \overline{\gtrless} n$ die Gleichheit

(34) $$s_1 s_2 \cdots s_m = \sigma_1 \sigma_2 \cdots \sigma_m \text{*)}.$$

Ist aber zweitens $m > n$, so sind die m Congruenzen (32) mit n Unbekannten völlig gleichbedeutend den m Gleichungen (33) mit $m + n$ Unbekannten, man kann daher auch in diesem Falle das Kriterium der Auflösbarkeit anwenden, wie vorher, und findet als nothwendige und hinreichende Bedingung für die Auflösbarkeit der Congruenzen (32) in diesem Falle die Gleichheit des grössten gemeinsamen Theilers für die zwei Systeme von Zahlen:

$$\varkappa^m, \ \varkappa^{m-1} d_1, \ \varkappa^{m-2} d_2, \ \cdots \varkappa^{m-n} d_n$$

und

$$\varkappa^m, \ \varkappa^{m-1} \delta_1, \ \varkappa^{m-2} \delta_2, \ \cdots \varkappa^{m-n} \delta_n, \ \varkappa^{m-n-1} \delta_{n+1}$$

d. h. die Gleichheit

$$\varkappa^{m-n} \cdot s_1 s_2 \cdots s_n = \varkappa^{m-n-1} \cdot \sigma_1 \sigma_2 \cdots \sigma_{n+1}$$

oder

$$s_1 s_2 \cdots s_n \cdot \varkappa = \sigma_1 \sigma_2 \cdots \sigma_n \cdot \sigma_{n+1}.$$

Da nun nach dem vorletzten Satze von nr. 6 des zweiten Capitels e_i durch ε_i und daher auch der grösste gemeinsame Theiler s_i von e_i und $\varkappa$ durch den grössten gemeinsamen Theiler σ_i von ε_i und $\varkappa$ theilbar ist, so folgt aus vorstehender Gleichung σ_{n+1} theilbar durch $\varkappa$ d. h. $\sigma_{n+1} = \varkappa$, und die Bedingungsgleichung erhält die Gestalt

(35) $$s_1 s_2 \cdots s_n = \sigma_1 \sigma_2 \cdots \sigma_n$$

und ist in Verbindung mit der Gleichung $\sigma_{n+1} = \varkappa$ oder der ihr gleichbedeutenden Bedingung, dass ε_{n+1}

*) S. hierzu und zu dem Folgenden Smith a. a. O. art. 17 und 18.

durch $\varkappa$ theilbar sei, zugleich die nothwendige und hinreichende Bedingung für die Auflösbarkeit der Congruenzen (32).

Ist nun diese, resp. die Bedingung (34) erfüllt, so ist in beiden Fällen die Anzahl der incongruenten Lösungen jederzeit

$$|A, \varkappa| = s_1 s_2 \cdots s_n.$$

Denn, ist $\xi_1, \xi_2, \cdots \xi_n$ eine bestimmte Lösung, so erhält man daraus offenbar $|A, \varkappa|$ incongruente Lösungen mittels der Formeln:

$$\xi_1 + x_1, \ \xi_2 + x_2, \ \cdots \xi_n + x_n, \tag{36}$$

wenn man für $x_1, x_2, \cdots x_n$ jede der $|A, \varkappa|$ incongruenten Lösungen der Congruenzen

$$A_\alpha \equiv 0 \ (\text{mod. } \varkappa) \tag{37}$$

setzt; und umgekehrt, wenn $\xi_1', \xi_2', \cdots \xi_n'$ irgend eine andere Lösung der Congruenzen (32) bedeutet, so ist sie, da

$$\xi_1' - \xi_1, \ \xi_2' - \xi_2, \ \cdots \xi_n' - \xi_n$$

die Congruenzen (37) erfüllen, mit einer der Lösungen (36) (mod. $\varkappa$) congruent.

5. Bevor wir dieses Capitel schliessen, ziehen wir aus der allgemeinen Grundlage unserer Untersuchungen noch ein paar für die Folge wichtige Folgerungen.

Führen wir, wie früher, statt der Linearformen A_α durch die Substitution

$$A_\alpha' = p_{\alpha 1} A_1 + p_{\alpha 2} A_2 + \cdots p_{\alpha m} A_m$$
$$(\alpha = 1, 2, \cdots m)$$

ebenso viel andere Linearformen A_α' ein, so leuchtet daraus, dass das System p ein Einheitssystem ist, sogleich ein, dass für jedes ganzzahlige System der Unbestimmten $x_1, x_2, \cdots x_n$ der grösste gemeinsame Theiler der ersteren gleich demjenigen der letzteren Formen ist. Gehen ferner durch die Substitution

$$x_\alpha = q_{\alpha 1} y_1 + q_{\alpha 2} y_2 + \cdots + q_{\alpha n} y_n$$
$$(\alpha = 1, 2, \cdots n)$$

die A_α' in die Linearformen B_α über, so wird der grösste gemeinsame Theiler der B_α für jedes Werthsystem der y gleich

dem grössten gemeinsamen Theiler der A'_α oder der A_α für das entsprechende Werthsystem der x sein. Indem nun p und q so gewählt werden, dass

$$B_1 = e_1 y_1, \; B_2 = e_2 y_2, \; \cdots B_r = e_r y_r, \; B_{r+1} = 0 \cdots B_m = 0$$

werden, und darauf $y_1 = 1$, die übrigen y beliebig genommen werden, erhalten die B_α den grössten gemeinsamen Theiler e_1 d. i. denselben grössten gemeinsamen Theiler, wie die sämmtlichen Coefficienten $a_{\alpha\beta}$.

Ist mithin d grösster gemeinsamer Theiler aller Zahlen $a_{\alpha\beta}$ des Systems a, so kann man $x_1, x_2, \cdots x_n$ so wählen, dass auch der grösste gemeinsame Theiler aller Formen

$$A_1, \; A_2, \; \cdots A_m$$

gleich d wird*).

Sind also z. B. die $2m$ Zahlen

$$a_1, a_2, \cdots a_m; \; b_1, b_2, \cdots b_m$$

ohne gemeinsamen Theiler, so lassen sich x, y so wählen, dass die m Ausdrücke

$$a_1 x + b_1 y, \; a_2 x + b_2 y, \; \cdots a_m x + b_m y$$

keinen gemeinsamen Theiler haben.

Wenn insbesondere nicht die sämmtlichen Ausdrücke

$$(38) \qquad a_\alpha b_\beta - a_\beta b_\alpha$$

verschwinden, lässt sich dabei $x = 1$, die Zahl y also so wählen, dass die Zahlen

$$(39) \qquad a_1 + b_1 y, \; a_2 + b_2 y, \; \cdots a_m + b_m y$$

ohne gemeinsamen Theiler sind. Auf diesen — aus dem Vorigen nicht unmittelbar fliessenden — Satz stützt sich Frobenius im Journ. f. Math. 86 S. 156 zum Beweise des ausgesprochenen allgemeinen Satzes. Er beweist jenen mittels der gleichen Principien, deren sich auch Smith bedient, folgendermassen. Jeder gemeinsame Theiler der Zahlen (39) müsste auch in

$$b_\beta(a_\alpha + b_\alpha y) - b_\alpha(a_\beta + b_\beta y)$$

*) S. bei Smith a. a. O. S. 314 einen Beweis dieses Satzes für den Fall $m < n$.

d. i. in allen Zahlen (38) aufgehen. Lässt sich also y so wählen, dass die erstgenannten keinen gemeinsamen Theiler haben mit dem grössten gemeinsamen Theiler δ der letzteren, so müssen sie überhaupt ohne gemeinsamen Theiler sein. Eine solche Wahl von y ist aber möglich, denn man kann allgemeiner y so wählen, dass die Zahlen (39) mit einer beliebig vorgeschriebenen Zahl $\varkappa$ keinen Theiler gemeinsam haben. In der That, sind $p, q, r \dots$ die Primfaktoren von $\varkappa$, so muss, da die $2m$ Zahlen a_α, b_α der Voraussetzung nach keinen gemeinsamen Theiler haben, wenigstens eine von ihnen durch p nicht theilbar sein; ist es a_α, so setze man

$$y \equiv 0 \pmod{p},$$

ist es b_α, so wähle man y (mod. p) so, dass etwa

$$a_\alpha + b_\alpha y \equiv 1 \pmod{p}$$

wird; man kann auf diese Weise y (mod. p) so bestimmen, dass eine der Zahlen (39) nicht durch p, in gleicher Weise (mod. q) so, dass eine von ihnen nicht durch q theilbar ist u. s. w., folglich auch (mod. $p\,q\,r \dots$) so, dass sie nicht sämmtlich einen Primfaktor von $\varkappa$ gemeinschaftlich haben, w. z. b. w.

Hieraus folgt speciell die Bemerkung, dass, wenn

$$a_1\ a_2 \cdots a_m$$

mehrere Zahlen sind, die zusammen mit $\varkappa$ keinen gemeinsamen Theiler haben, sich andere ihnen (mod. $\varkappa$) congruente Zahlen

$$\alpha_1\ \alpha_2 \cdots \alpha_m$$

angeben lassen, die überhaupt keinen gemeinsamen Theiler haben. Denn zunächst darf man voraussetzen, dass sie nicht sämmtlich gleich sind, weil man sie sonst durch ungleiche ihnen (mod. $\varkappa$) congruente ersetzen könnte. Wählt man dann sämmtliche Zahlen b_α gleich $\varkappa$, so sind die Zahlen (38) nicht alle Null, der vorige Satz wird anwendbar und y kann so gewählt werden, dass die Zahlen

$$\alpha_1 = a_1 + \varkappa y,\ \alpha_2 = a_2 + \varkappa y,\ \cdots \alpha_m = a_m + \varkappa y$$

ohne gemeinsamen Theiler sind.

Auf diesen einfachen Satz gründen wir den Beweis eines

anderen Satzes, dessen wir in der Folge mehrfach bedürfen. Ist

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{matrix}$$

ein quadratisches Zahlensystem a, dessen Determinante *congruent* 1 (mod. $\varkappa$) ist, so lässt sich ein anderes angeben, dessen Elemente denjenigen des ersteren congruent sind, dessen Determinante aber *gleich* 1 ist. Da dieser Satz für $m = 1$ selbstverständlich ist, werden wir ihn beweisen, wenn wir feststellen, dass er für m gilt, falls er bereits für $m - 1$ richtig ist. Nun folgt zunächst aus der Voraussetzung, dass die Zahlen $a_{11}, a_{21}, \cdots a_{m1}$ keinen mit $\varkappa$ gemeinsamen Theiler haben können; folglich lassen sich andere ihnen (mod. $\varkappa$) congruente: $\alpha_{11}, \alpha_{21}, \cdots \alpha_{m1}$ angeben, welche überhaupt ohne gemeinsamen Theiler sind, und nunmehr nach Cap. 3 nr. 5 ein System α:

$$\begin{matrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mm} \end{matrix}$$

aufstellen, dessen Determinante gleich 1 ist. Setzt man das reciproke System α^{-1} mit dem Systeme a zusammen, so erhält man ein drittes System β:

$$\begin{matrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mm}, \end{matrix}$$

in welchem offenbar

$$\beta_{11} \equiv 1, \ \beta_{21} \equiv 0 \cdots \beta_{m1} \equiv 0 \ (\text{mod. } \varkappa)$$

sind, während seine Determinante und daher auch die Determinante von

$$\begin{matrix} \beta_{22} & \cdots & \beta_{2m} \\ \cdot & \cdot & \cdot \\ \beta_{m2} & \cdots & \beta_{mm} \end{matrix}$$

der Einheit congruent ist. Wenn man nun die Elemente des letzteren Systems vom $m - 1^{\text{ten}}$ Grade, was nach der Voraus-

setzung geschehen kann, durch solche andere, ihnen (mod. $\varkappa$) congruente

$$\begin{matrix} b_{22} & \cdots & b_{2m} \\ \cdot & \cdot & \cdot \\ b_{m2} & \cdots & b_{mm} \end{matrix}$$

ersetzt, dass deren Determinante $|b_{i\varkappa}| = 1$ wird, und man wählt

$$b_{11} = 1,\ b_{21},\ \cdots b_{m1} \text{ gleich } 0$$
$$b_{12} \equiv \beta_{12},\ \cdots b_{1m} \equiv \beta_{1m} \pmod{\varkappa},$$

so ist offenbar das System b:

$$\begin{matrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mm} \end{matrix}$$

dem System β (mod. $\varkappa$) congruent und seine Determinante gleich 1. Das letztere gilt mithin auch für das zusammengesetzte System $\alpha \cdot b$. Da zudem

$$\beta = \alpha^{-1} \cdot a \quad \text{also} \quad a = \alpha \cdot \beta$$

ist, so ist ersichtlich

$$a \equiv \alpha \cdot b$$

und das System $\alpha \cdot b$ genügt folglich allen Anforderungen des Satzes*).

6. Noch sei folgender Satz hier mitgetheilt, der mit dem Gegenstande der letzten Capitel nahe verwandt ist und auf den wir später zu verweisen haben werden.

Jede rationale Transformation d. i. jede Transformation mit rationalen Coefficienten kann in solche zerlegt werden, deren Modulus und Generalnenner nur eine einzige Primzahl enthalten. — Da man, wenn ein Generalnenner vorhanden ist, ihn offenbar durch successive

*) Der hier gegebene Beweis des Satzes ist nach Minkowski, Untersuchungen über quadratische Formen, in Acta Math. Bd. 7. Einen anderen Beweis, der sich unmittelbar auf die Reduktionsformel (15) des Cap. 2 stützt, s. bei Smith, mém. sur la représentation des nombres par des sommes de cinq carrés, in Mém. des Savants Etrangers 29, S 16.

Substitutionen $x_i = \frac{x_i'}{p^\alpha}$ einführen kann, braucht man den Satz nur für ganzzahlige Transformationen zu erweisen. Jede solche aber setzt sich aus einer Substitution (P) von der Form:

$$\begin{aligned} x_1 &= p_1^1 y_1 \\ x_2 &= p_2^1 y_1 + p_2^2 y_2 \\ &\cdots\cdots\cdots \\ x_n &= p_n^1 y_1 + p_n^2 y_2 + \cdots + p_n^n y_n \end{aligned}$$

und einer unimodularen zusammen. Nun ist erstens das Produkt zweier analogen Substitutionen $(P), (Q)$ wieder eine mit (P) analoge Substitution (R), in welcher

$$r_h^h = p_h^h \cdot q_h^h$$

$$r_h^{h-d} = \sum_{\delta=0}^{d} p_h^{h-\delta} \cdot q_{h-\delta}^{h-d}$$

$$(d = 1, 2, \cdots h-1)$$

ist. Zweitens kann jede mit (P) analoge Substitution (R) in ein Produkt zweier anderen $(P), (Q)$ zerlegt werden, sobald man die Elemente r_h^h so in zwei Faktoren p_h^h, q_h^h zerlegt, dass jedes p_h^h prim ist zu $q_1^1, q_2^2, \cdots q_{h-1}^{h-1}$. Denn dann lassen sich zuerst die Elemente p_h^{h-d} durch die Congruenzen

$$p_h^{h-d} \equiv \frac{r_h^{h-d} - \sum_{\delta=1}^{d-1} p_h^{h-\delta} \cdot q_{h-\delta}^{h-d}}{q_{h-d}^{h-d}} \pmod{p_h^h}$$

und dann

$$q_h^{h-d} = \frac{r_h^{h-d} - \sum_{\delta=1}^{d} p_h^{h-\delta} \cdot q_{h-\delta}^{h-d}}{p_h^h}$$

wählen.

Werden beispielsweise die p_h^h als die höchsten in den r_h^h aufgehenden Potenzen einer Primzahl gewählt, so kommt man zu der behaupteten Zerlegung der rationalen Transformation (s. Journ. f. Math. 106 S. 20).

Fünftes Capitel.

Algebraisches über quadratische Formen.

1. Wir beginnen dieses Capitel, indem wir aus der Theorie der Elementartheiler einige auf die der bilinearen Formen bezügliche Folgerungen herleiten.

Wenn

$$F_a = \sum a_{\alpha\beta} x_\alpha y_\beta \qquad (\alpha = 1, 2, \cdots m;\ \beta = 1, 2, \cdots n) \tag{1}$$

eine bilineare Form mit m Unbestimmten $x_1, x_2, \cdots x_m$ und n Unbestimmten $y_1, y_2, \cdots y_n$ ist, so kann man sie transformiren, indem man für die Unbestimmten durch die Substitutionen

$$\left\{\begin{array}{l} x_\alpha = p_{1\alpha} x_1' + p_{2\alpha} x_2' + \cdots + p_{m\alpha} x_m' \qquad (\alpha = 1, 2, \cdots m) \\ y_\beta = q_{\beta 1} y_1' + q_{\beta 2} y_2' + \cdots + q_{\beta n} y_n' \qquad (\beta = 1, 2, \cdots n) \end{array}\right. \tag{2}$$

ebenso viele andere einführt. Die so entstehende transformirte Form

$$F_b = \sum b_{\gamma\delta} x_\gamma' y_\delta' \qquad (\gamma = 1, 2, \cdots m;\ \delta = 1, 2, \cdots n) \tag{3}$$

hat die Coefficienten

$$b_{\gamma\delta} = \sum_{\alpha,\beta} p_{\gamma\alpha} \cdot a_{\alpha\beta} \cdot q_{\beta\delta}. \tag{4}$$

Bezeichnet man also mit a, b die aus den Coefficienten beider Formen gebildeten Zahlensysteme vom Typus $m \cdot n$, mit p, q die quadratischen Zahlensysteme

$$p_{\gamma 1}, p_{\gamma 2}, \cdots p_{\gamma m} \quad (\gamma = 1, 2, \cdots m) \qquad \text{und} \qquad q_{\beta 1}, q_{\beta 2}, \cdots q_{\beta n}, \quad (\beta = 1, 2, \cdots n)$$

so findet sich die Beziehung

$$b = p \cdot a \cdot q. \tag{5}$$

Setzen wir voraus, dass sowohl die Coefficienten der Form F_a als auch die der Substitutionen (2) ganzzahlig sind, so lehrt diese Beziehung, dass das System b unter dem Systeme

a enthalten, insbesondere, wenn p, q Einheitssysteme sind, ihm äquivalent ist. Wir sagen deshalb entsprechend: die bilineare Form F_b sei unter der Form F_a enthalten, resp., wenn sie durch unimodulare Substitutionen (2) aus F_a entsteht, sie sei F_a äquivalent. Die nothwendige und hinreichende Bedingung für die Aequivalenz der beiden ganzzahligen Formen F_a und F_b ist hiermit nach nr. 4 des zweiten Capitels die Bedingung, dass ihre Coefficientensysteme a, b gleichen Rang und gleiche Elementartheiler haben. — Conjugirte Formen F_a und F_a' sind folglich stets einander äquivalent. — Die Bedingungen des Enthaltenseins von F_b unter F_a lehrt der allgemeinere in jener nr. ausgesprochene Satz. Diesem zufolge müssen die Formen F_a, F_b, damit sie gegenseitig unter einander enthalten sind, gleichen Rang und gleiche Elementartheiler haben. Man kann daher die Aequivalenz zweier Formen auch so definiren: Zwei Formen heissen äquivalent, wenn jede unter der andern enthalten ist.

Da man die Einheitssysteme p_0, q_0 so wählen kann, dass

$$p_0 \cdot a \cdot q_0 = E \tag{6}$$

wird, wo, wenn r den Rang von a bedeutet, E die Form hat:

$$\begin{matrix} e_1 & 0 & \cdots & 0 & 0 & \cdots \\ 0 & e_2 & \cdots & 0 & 0 & \cdots \\ . & . & . & . & . & . \\ 0 & 0 & \cdots & e_r & 0 & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots \\ & & . & & . & ., \end{matrix}$$

so lässt sich die Form F_a durch geeignete unimodulare Substitutionen in die äquivalente Form

$$e_1 x_1' y_1' + e_2 x_2' y_2' + \cdots + e_r x_r' y_r' \tag{7}$$

überführen, die wir ihre Reducirte nennen wollen. Aequivalente ganzzahlige Formen F_a, F_b sind demgemäss durch den Umstand charakterisirt, dass ihre Reducirten identisch sind. Betrachten wir insbesondere den Fall, auf den wir uns bald ausschliesslich beschränken werden, dass $m = n = r$ ist, so sind die Coefficientensysteme der

Formen quadratische Systeme und aus der Gleichung (6) geht die andere

$$A = d_n \tag{8}$$

hervor. **Aequivalente Formen haben also alsdann dieselbe Determinante.**

Denkt man sich daher alle unter einander äquivalenten Formen in eine **Classe** zusammengefasst, so zerfällt die Gesammtheit aller Formen mit derselben Determinante D offenbar in so viel Classen, als es Reducirte mit der Determinante D giebt. In jeder reducirten Form mit dieser Determinante muss aber

$$D = e_1 e_2 \cdots e_n$$

oder, da $\frac{e_\varkappa}{e_{\varkappa-1}}$ eine ganze Zahl $f_\varkappa$, folglich

$$e_1 = f_1, \; e_2 = f_1 f_2, \; \cdots e_n = f_1 f_2 \cdots f_n$$

ist, muss

$$D = f_1^n \cdot f_2^{n-1} \cdots f_{n-1}^2 \cdot f_n \tag{9}$$

sein. Die Anzahl $h(D)$ nicht äquivalenter bilinearer Formen

$$\sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha y_\beta \tag{10}$$

mit der Determinante D wird folglich gleich der Zahl sein, welche angiebt, auf wieviel Arten D in der Gestalt (9) darstellbar ist. Offenbar ist demnach

$$h(D) = h(D') \cdot h(D''),$$

wenn $D = D'D''$ eine Zerlegung von D in zwei relativ prime Faktoren D', D'' ist. Ist aber a^α eine der Primzahlpotenzen, aus denen D besteht, so ist $h(a^\alpha)$ d. i. die Zahl, welche angiebt, wie oft a^α in der Gestalt (9):

$$a^\alpha = a^{n\alpha_1 + (n-1)\alpha_2 + \cdots + 2\alpha_{n-1} + \alpha_n}.$$

oder α in der Gestalt

$$\alpha = n\alpha_1 + (n-1)\alpha_2 + \cdots + 2\alpha_{n-1} + \alpha_n$$

darstellbar ist, wie sogleich zu übersehen, der Coefficient h_α von x^α in der Reihenentwickelung

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^n)} = h_0 + h_1 x + h_2 x^2 + \cdots$$

Und somit findet sich, wenn

$$D = \pm a^{\alpha} b^{\beta} c^{\gamma} \cdots$$

gesetzt wird, die Anzahl $h(D)$ nicht äquivalenter bilinearer Formen von der Gestalt (10) und der Determinante D durch die Formel:

$$h(D) = h_{\alpha} \cdot h_{\beta} \cdot h_{\gamma} \cdots, \tag{11}$$

welche lehrt, dass sie nur von der *Häufigkeit* der Primfaktoren von D, nicht von ihrem *Werthe* bestimmt ist.

2. Die Theorie der Elementartheiler, wie wir sie im zweiten Capitel auseinandergesetzt haben, ist keineswegs auf den für unsere Zwecke ausschliesslich festgehaltenen Fall beschränkt, wo die Elemente der Zahlensysteme reelle ganze Zahlen sind. Sie kann z. B. in genau derselben Weise entwickelt werden, wenn diese Elemente ganze Funktionen einer Veränderlichen λ mit beliebigen Coefficienten sind, und es bedarf fast nur des Ersatzes des Ausdrucks „ganze Zahl" durch den anderen „ganze Funktion von λ", um aus den entwickelten Sätzen die dann giltigen zu erhalten. So sind die mit d_x bezeichneten grössten gemeinsamen Theiler aller Determinanten x^{ten} Grades eines Systems a sowie seine Elementartheiler e_x und deren Quotienten $\frac{e_x}{e_{x-1}}$ alsdann ganze Funktionen von λ; und wenn man zwei bilineare Formen F_a, F_b, deren Coefficienten ganze Funktionen von λ sind, äquivalent nennt, wenn eine von ihnen in die andere übergeht durch zwei Substitutionen von der Gestalt (2), deren Coefficienten ganze Funktionen von λ sind, deren Determinante aber ein von λ unabhängiger, von Null verschiedener Werth ist, so findet man als nothwendige und hinreichende Bedingung der Aequivalenz wieder die Gleichheit der Elementartheiler beider Formen. Denkt man sich die ganzen Funktionen von λ, welche die Zeichen d_x vorstellen, in ihre Linearfaktoren zerlegt, bezeichnet mit $(\lambda - l)^{\delta_x}$ die höchste Potenz eines solchen Linearfaktors $\lambda - l$, welche in d_x aufgeht, und setzt

$$\delta_x - \delta_{x-1} = \varepsilon_x,$$

so ist $(\lambda - l)^{e_\varkappa}$ die höchste Potenz dieses Linearfaktors, welche in $c_\varkappa$ enthalten ist. Frobenius nennt die Faktoren $(\lambda - l)^{e_\varkappa}$ die einfachen Elementartheiler, während Weierstrass für diese Theiler den Ausdruck „Elementartheiler" überhaupt gebraucht. Nun werden aber zwei Formen, welche gleiche Elementartheiler $e_\varkappa$ haben, offenbar auch dieselben einfachen Elementartheiler haben und auch umgekehrt. Der ausgesprochene Satz behält mithin seine Giltigkeit auch dann, wenn darin der Ausdruck „Elementartheiler" im Weierstrass'schen Sinne genommen wird.

Da wir diese Verhältnisse nur soweit untersuchen wollen, als sie mit unserem Gegenstande verbunden sind, beschränken wir uns, wie von nun an überhaupt, auf den Fall $m = n = r$.

Seien dann

$$F_a = \sum a_{\alpha\beta}\, x_\alpha\, y_\beta, \quad F_b = \sum b_{\alpha\beta}\, x_\alpha\, y_\beta \qquad (\alpha, \beta = 1, 2, \cdots n) \tag{12}$$

zwei bilineare Formen mit $2n$ Veränderlichen, deren Coefficienten ganze Funktionen ersten Grades von λ sind, sodass man für ihre Systeme die Gleichungen

$$a = \lambda a^{(0)} + a^{(1)}, \ b = \lambda b^{(0)} + b^{(1)}$$

ansetzen darf, wo nun die Elemente der Zahlensysteme $a^{(0)}$, $a^{(1)}$, $b^{(0)}$, $b^{(1)}$ von λ unabhängig sind. Setzen wir voraus, dass die Determinanten $A^{(0)}$, $B^{(0)}$ von $a^{(0)}$, $b^{(0)}$ nicht Null sind, so haben beide Systeme den Rang n, denn ihre Determinanten sind dann nicht für jedes λ gleich Null. Sind ferner die Elementartheiler beider Formen einander gleich, so sind diese dem Gesagten zufolge äquivalent und es giebt folglich Substitutionen (2), deren Coefficienten ganze Funktionen von λ, deren Determinanten aber von λ unabhängige, nicht verschwindende Werthe sind, so beschaffen, dass

$$p \cdot a \cdot q = b \tag{13}$$

ist. Wir wollen zeigen, dass man die Elemente der Systeme p, q als von λ unabhängig voraussetzen darf.

Zunächst werden jedenfalls auch die reciproken Systeme p^{-1}, q^{-1} Elemente haben, welche ganze Funktionen von λ

sind, während ihre Determinanten von λ unabhängig und von Null verschieden sind; aus (13) aber folgt

(14) $$p \cdot a = b \cdot q^{-1}.$$

Wenn nun die Elemente von p abhängig von λ sind und λ^c ist die höchste in ihnen vorkommende Potenz von λ, sodass man

$$p = p_0 \lambda^c + p_1 \lambda^{c-1} + \cdots + p_c$$

setzen darf, wo nun die Elemente der Systeme $p_0, p_1, \cdots p_c$ von λ unabhängig sind, so lässt sich stets ein System

$$\varpi = \varpi_0 \lambda^{c-1} + \varpi_1 \lambda^{c-2} + \cdots + \varpi_{c-1}$$

und ein von λ unabhängiges System ϱ so bestimmen, dass

(15a) $$p = b \cdot \varpi + \varrho$$

wird. Denn nach den Regeln des ersten Capitels werden hierzu folgende Bedingungsgleichungen zu erfüllen sein:

$$\begin{aligned} p_0 &= b^{(0)} \cdot \varpi_0 \\ p_1 &= b^{(0)} \cdot \varpi_1 + b^{(1)} \cdot \varpi_0 \\ p_2 &= b^{(0)} \cdot \varpi_2 + b^{(1)} \cdot \varpi_1 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ p_c &= b^{(1)} \cdot \varpi_{c-1} + \varrho, \end{aligned}$$

deren c ersten man, da B_0 von Null verschieden vorausgesetzt worden, nach nr. 4 des ersten Capitels durch ganz bestimmte Zahlensysteme $\varpi_0, \varpi_1, \cdots \varpi_{c-1}$ genügen kann, während dann die letzte auch ϱ unzweideutig definirt.

Aehnlicherweise darf man

(15b) $$q = \varkappa \cdot b + \sigma$$

und entsprechend

(15c) $$p^{-1} = a\varpi^{(1)} + \varrho^{(1)}$$

(15d) $$q^{-1} = \varkappa^{(1)} a + \sigma^{(1)}$$

setzen, wo $\sigma, \varrho^{(1)}, \sigma^{(1)}$ von λ unabhängig sind. Alsdann nimmt aber die Beziehung (14) die Gestalt an:

$$b(\varpi - \varkappa^{(1)})a = b\sigma^{(1)} - \varrho a.$$

Da nun $A^{(0)}, B^{(0)}$ von Null verschieden sind, ein Produkt $b^{(0)} \cdot c$ oder $c \cdot a^{(0)}$ nach der eben angezogenen nr. 4 des ersten Capitels also nur zugleich mit c verschwinden kann, so erkennt

man ohne Mühe, dass, wenn $\varpi - \varkappa^{(1)}$ nicht Null wäre, die linke Seite der vorigen Gleichung in Bezug auf λ mindestens vom 2. Grade sein würde, während die rechte höchstens vom 1. Grade ist; somit findet sich

(16) $$b \cdot \sigma^{(1)} = \varrho \cdot a$$

Andererseits ist $q \cdot q^{-1} = e$ d. h. nach den Formeln (15)

$$q \cdot \varkappa^{(1)} \cdot a + \varkappa \cdot b \cdot \sigma^{(1)} = e - \sigma \cdot \sigma^{(1)}$$

oder wegen (16)

$$(q \cdot \varkappa^{(1)} + \varkappa \cdot \varrho) \cdot a = e - \sigma \cdot \sigma^{(1)},$$

und hieraus schliesst man mittels der gleichen Erwägung

$$q \cdot \varkappa^{(1)} + \varkappa \cdot \varrho = 0, \; e - \sigma \cdot \sigma^{(1)} = 0$$

d. h. $\sigma^{(1)} = \sigma^{-1}$ und also wegen (16)

(17) $$b = \varrho \cdot a \cdot \sigma$$

also auch

$$b^{(0)} = \varrho \cdot a^{(0)} \cdot \sigma,$$

weshalb die Determinanten der Systeme ϱ, σ von Null verschieden sein müssen. Aus der auf solche Weise erhaltenen Gleichung (17) ziehen wir folgenden Schluss*):

Haben die beiden Formen F_a, F_b, deren Coefficienten lineare ganze Funktionen von λ sind, dieselben Elementartheiler, sind sie also in der oben angegebenen Bedeutung einander äquivalent, so kann man die eine in die andere durch zwei Substitutionen überführen, deren Coefficienten von λ unabhängig und deren Determinanten von Null verschieden sind. Ist aber umgekehrt letzteres der Fall, so sind F_a, F_b offenbar auch in der obigen Bedeutung äquivalent. Man darf demnach für Formen von der Art der Formen (12) den Begriff der Aequivalenz auch dahin fassen: dass zwei solche Formen äquivalent zu nennen sind, wenn eine in die andere durch zwei *von λ unabhängige* Substitutionen, deren Determinanten von Null verschieden sind, übergeführt werden kann. Und hieraus ergiebt sich dann der zuerst von Weierstrass bewiesene Fundamentalsatz**):

---

*) S. Frobenius, Journ. f. Math. 86 S. 205.

**) S. Monatsberichte der Berl. Akad. v Jahre 1868 S. 310.

Sind

$$\lambda F_{a_0} + F_{a_1} \text{ und } \lambda F_{b_0} + F_{b_1}$$

zwei aus den Formen

$$F_{a_0} = \sum a_{\alpha\beta}^{(0)} x_\alpha y_\beta, \quad F_{a_1} = \sum a_{\alpha\beta}^{(1)} x_\alpha y_\beta$$
$$F_{b_0} = \sum b_{\alpha\beta}^{(0)} x_\alpha y_\beta, \quad F_{b_1} = \sum b_{\alpha\beta}^{(1)} x_\alpha y_\beta$$

zusammengesetzte *Schaaren von bilinearen Formen*, und werden diese beiden Schaaren einander äquivalent genannt, wenn die eine in die andere durch zwei von λ unabhängige Substitutionen übergeht, deren Determinanten von Null verschieden sind, so ist die nothwendige und hinreichende Bedingung ihrer Aequivalenz die Gleichheit ihrer Elementartheiler.

3. Bisher haben wir bei der Transformation der bilinearen Formen und der Definition ihrer Aequivalenz die angewandten Substitutionen im allgemeinen ganz beliebig gedacht. Man kann sie aber dabei auch irgend welchen Bedingungen unterwerfen, z. B. — was für unsere Zwecke der einzige in Frage kommende Fall ist — verlangen, dass sie für beide Reihen von Veränderlichen übereinstimmen oder, wie man sagt, dass diese Veränderlichen cogredient sein sollen*). Alsdann hört die zuvor angegebene Aequivalenzbedingung sowie die darauf gegründete Reduktion der Formen auf, zutreffend zu sein. Wir beschränken uns, wie schon bemerkt, von nun an auf den Fall $m = n$, setzen also die bilinearen Formen stets von der

*) Die Transformationen der bilinearen Formen, insbesondere diejenigen, welche eine solche Form in sich selbst transformiren, sind sowohl im Allgemeinen, als für verschiedene Voraussetzungen über die Beschaffenheit der anzuwendenden Substitutionen in den Arbeiten von Frobenius (über lineare Substitutionen und bilineare Formen, J. f. Math. 84), Kronecker (über Schaaren von quadratischen und bilinearen Formen, und: über die congruenten Transformationen der bilinearen Formen, in Berl. Monatsberichte 1874), Voss (über die cogredienten Transformationen einer bilinearen Form in sich selbst, Abhh. der Kgl. Bayerischen Ak. der Wiss. Bd. 17 S. 235; über die conjugirte Transformation einer bilinearen Form in sich selbst, Sitzungsber. derselben Akademie, 1889) u. A. ausführlich behandelt worden; hier kann nur auf diese Arbeiten verwiesen werden.

Gestalt

$$F_a = \sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha y_\beta \tag{18}$$

voraus, lassen jedoch die Coefficienten der Formen sowohl wie der Substitutionen einstweilen völlig beliebige Zahlen bedeuten, nur dass wir meist

$$a_{\alpha\beta} = a_{\beta\alpha} \tag{19}$$

d. h. wie man sagt, die bilineare Form als symmetrisch voraussetzen werden. Bilineare Formen, bei welchen im Gegentheil

$$a_{\alpha\beta} = -a_{\beta\alpha} \tag{20}$$

ist, werden alternirend genannt. Sollen nun die Substitutionen (2), durch welche die Form (18) transformirt wird, übereinstimmen, so muss allgemein

$$p_{\alpha\beta} = q_{\beta\alpha} \text{ d. h. } p = q'$$

sein und folglich erhält man für die transformirte Form

$$F_b = \sum_{(\gamma, \delta = 1, 2, \cdots n)} b_{\gamma\delta} x_\gamma' y_\delta' \tag{21}$$

die Relation

$$b = q' \cdot a \cdot q, \tag{22}$$

während die Gleichung (4) die besondere Gestalt

$$b_{\gamma\delta} = \sum_{\alpha, \beta} q_{\alpha\gamma} \cdot a_{\alpha\beta} \cdot q_{\beta\delta} \tag{23}$$

annimmt, und, so oft die Gleichheit (19) erfüllt ist, die Gleichheit

$$b_{\gamma\delta} = b_{\delta\gamma}$$

ergiebt; die transformirte Form ist mithin dann wieder symmetrisch.

Werden insbesondere dann die Variabeln x_α mit den y_α, desgleichen die x_α' mit den y_α' als identisch angenommen, so werden die bilinearen Formen F_a, F_b zu quadratischen Formen

$$\sum_{\alpha, \beta} a_{\alpha\beta} x_\alpha x_\beta \tag{24}$$

und

$$\sum_{\gamma,\delta} b_{\gamma\delta}\, x_\gamma' x_\delta' \tag{25}$$

resp., und die erstere verwandelt sich in die letztere durch die *eine* Substitution

$$x_\alpha = q_{\alpha 1} x_1' + q_{\alpha 2} x_2' + \cdots + q_{\alpha n} x_n'; \quad (\alpha = 1, 2, \cdots n) \tag{26}$$

zwischen dem Systeme der Coefficienten der transformirten und der ursprünglichen quadratischen Form besteht, wie zuvor, die Relation (22) oder die dieselbe aussprechenden $n \cdot n$ Gleichungen (23). Aus letzterem Umstande ersieht man aber auch umgekehrt, dass, wenn die quadratische Form (24) durch die Substitution (26) in die quadratische Form (25) übergeht, sich die symmetrische bilineare Form F_a durch die gleichlautenden Transformationen

$$\begin{cases} x_\alpha = q_{\alpha 1} x_1' + q_{\alpha 2} x_2' + \cdots + q_{\alpha n} x_n' \\ y_\alpha = q_{\alpha 1} y_1' + q_{\alpha 2} y_2' + \cdots + q_{\alpha n} y_n' \\ \quad (\alpha = 1, 2, \cdots n) \end{cases} \tag{27}$$

in die symmetrische bilineare Form F_b verwandelt. Beide Transformationen sind demnach mit einander, nämlich mit der Transformation des Zahlensystems a mittels der Formel (22) gleichbedeutend; mit dieser werden wir uns daher nun weiter beschäftigen.

4. Heisst wieder Q die Determinante oder der Modulus der Substitution (26), welcher stets als von Null verschieden gedacht werden soll, nennt man $Q_{\alpha\beta}$ das zu $q_{\alpha\beta}$ adjungirte Element der Determinante Q und setzt

$$\frac{Q_{\alpha\beta}}{Q} = \gamma_{\alpha\beta}, \tag{28}$$

so bilden die Gleichungen

$$x_\alpha' = \gamma_{1\alpha} x_1 + \gamma_{2\alpha} x_2 + \cdots + \gamma_{n\alpha} x_n \quad (\alpha = 1, 2, \cdots n) \tag{29}$$

die Auflösung der Gleichungen (26) oder die reciproke Substitution, und es ist

$$\gamma = q^{-1}. \tag{30}$$

Durch diese Substitution verwandelt sich rückwärts die quadratische Form (25) in die ursprüngliche (24), denn aus (22)

folgt, da $\gamma' = (q^{-1})' = q'^{-1}$ ist,

(31) $$a = \gamma' \cdot b \cdot \gamma.$$

Betrachtet man neben den durch die Gleichungen (26) oder (29) mit einander verbundenen zwei Variabelnsystemen

(32) $$x_1, x_2, \cdots x_n; \quad x_1', x_2', \cdots x_n'$$

zwei andere:

(33) $$y_1, y_2, \cdots y_n; \quad y_1', y_2', \cdots y_n',$$

welche durch die Gleichungen

(34) $$y_\alpha' = q_{1\alpha} y_1 + q_{2\alpha} y_2 + \cdots + q_{n\alpha} y_n \quad (\alpha = 1, 2, \cdots n)$$

also

(35) $$y_\alpha = \gamma_{\alpha 1} y_1' + \gamma_{\alpha 2} y_2' + \cdots + \gamma_{\alpha n} y_n' \quad (\alpha = 1, 2, \cdots n)$$

unter einander verbunden sind, so werden die Variabeln (33) **contragredient** zu den Variabeln (32) genannt*). Indem man die letzten Gleichungen der Reihe nach mit $x_1, x_2, \cdots x_n$ multiplicirt und dann addirt, erschliesst man mittels der Formeln (5) des ersten Capitels sogleich die wichtige Beziehung:

(36) $$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = x_1' y_1' + x_2' y_2' + \cdots + x_n' y_n'.$$

Wenn umgekehrt diese Beziehung erfüllt ist, während die x_α' mit den x_α durch die Gleichungen (26) und zugleich die y_α' linear mit den y_α durch Gleichungen von der Form

(37) $$y_\alpha' = c_{1\alpha} y_1 + c_{2\alpha} y_2 + \cdots + c_{n\alpha} y_n \quad (\alpha = 1, 2, \cdots n)$$

verbunden sind, so nimmt sie vermöge dieser Verbindungen die Gestalt an:

$$\sum_{\alpha, \gamma} q_{\alpha\gamma} x_\gamma' y_\alpha = \sum_{\alpha, \gamma} c_{\alpha\gamma} x_\gamma' y_\alpha,$$

woraus sogleich $c_{\alpha\gamma} = q_{\alpha\gamma}$ d. h. die Identität der Gleichungen (37) mit den Gleichungen (34) hervorgeht. **Contragrediente Substitutionen** (oder **Variabeln**) sind also dadurch

*) Nach Gauss nennt man die durch die Gleichungen (34), (35) ausgesprochenen Substitutionen die **transponirten Substitutionen** zu (26) resp. (29).

charakterisirt, dass sie die bilineare Form

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

ungeändert lassen.

Setzt man die quadratische Form

$$\sum_{\alpha, \beta} a_{\alpha \beta} x_\alpha x_\beta = f(x_i), \tag{38}$$

so folgt, dem Euler'schen Satze von den homogenen Funktionen entsprechend, die Identität:

$$f(x_i) = x_1 \cdot \frac{1}{2} \frac{\partial f(x_i)}{\partial x_1} + \cdots + x_n \cdot \frac{1}{2} \frac{\partial f(x_i)}{\partial x_n}. \tag{39}$$

Wird ferner zur Abkürzung

$$X_\alpha = \frac{1}{2} \frac{\partial f(x_i)}{\partial x_\alpha} \tag{40}$$

gesetzt, so findet man die n Gleichungen

$$X_\alpha = a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha n} x_n \tag{41}$$
$$(\alpha = 1, 2, \cdots n)$$

und bei Anwendung der in nr. 1 und 2 des ersten Capitels eingeführten Bezeichnungen ihre Auflösung in der Gestalt:

$$x_\gamma = \alpha_{1\gamma} X_1 + \alpha_{2\gamma} X_2 + \cdots + \alpha_{n\gamma} X_n. \tag{42}$$
$$(\gamma = 1, 2, \cdots n)$$

Die Determinante A der Gleichungen (41) oder des Zahlensystems a wird die Determinante der quadratischen Form $f(x_i)$ — nach Gauss — genannt. Nun sind, wenn

$$Y_\alpha = a_{1\alpha} y_1 + a_{2\alpha} y_2 + \cdots + a_{n\alpha} y_n$$
$$(\alpha = 1, 2, \cdots n)$$

also

$$y_\gamma = \alpha_{\gamma 1} Y_1 + \alpha_{\gamma 2} Y_2 + \cdots + \alpha_{\gamma n} Y_n$$
$$(\gamma = 1, 2, \cdots n)$$

gesetzt wird, die Variabeln Y_α den x_α contragredient, zugleich aber kann man wegen (19)

$$Y_\alpha = \frac{1}{2} \frac{\partial f(y_i)}{\partial y_\alpha}$$

setzen. Nach (36) erhält man also die Gleichung

$$(43)\qquad x_1 \cdot \frac{1}{2}\frac{\partial f(y_i)}{\partial y_1} + \cdots + x_n \cdot \frac{1}{2}\frac{\partial f(y_i)}{\partial y_n}$$
$$= y_1 \cdot \frac{1}{2}\frac{\partial f(x_i)}{\partial x_1} + \cdots + y_n \cdot \frac{1}{2}\frac{\partial f(x_i)}{\partial x_n}$$

d. h. den Satz: Sind

$$x_1, x_2, \cdots x_n;\ y_1, y_2, \cdots y_n$$

irgend zwei Systeme von n Werthen, so bleibt der Ausdruck

$$x_1 \cdot \frac{1}{2}\frac{\partial f(y_i)}{\partial y_1} + x_2 \cdot \frac{1}{2}\frac{\partial f(y_i)}{\partial y_2} + \cdots + x_n \cdot \frac{1}{2}\frac{\partial f(y_i)}{\partial y_n}$$

ungeändert, wenn man die beiden Werthsysteme mit einander vertauscht.

5*). In fast allen Theilen der Mathematik und so auch in der Theorie der bilinearen und der quadratischen Formen tritt die Aufgabe auf, lineare Gleichungen von folgender Gestalt:

$$(44)\qquad \lambda \cdot y_\alpha = a_{\alpha 1} y_1 + a_{\alpha 2} y_2 + \cdots + a_{\alpha n} y_n$$
$$(\alpha = 1, 2, \cdots n)$$

aufzulösen. Sie haben nur die einzige Auflösung

$$y_1 = 0,\ y_2 = 0,\ \cdots y_n = 0,$$

es sei denn, dass die Grösse λ der Gleichung

$$(45)\qquad A(\lambda) = \begin{vmatrix} a_{11} - \lambda, & a_{12}, & \cdots & a_{1n} \\ a_{21}, & a_{22} - \lambda, & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1}, & a_{n2}, & \cdots & a_{nn} - \lambda \end{vmatrix} = 0$$

genügt. Diese, für das Vorhandensein anderer Auflösungen erforderliche Bedingungsgleichung soll die Fundamental- oder charakteristische Gleichung der Form F_a oder des Zahlensystems a genannt werden. Ihre Wurzeln seien $\lambda_1, \lambda_2, \cdots \lambda_n$. Ausführlich geschrieben hat sie die Gestalt

$$(45\text{a})\qquad (-\lambda)^n + A_1 \cdot (-\lambda)^{n-1} + \cdots$$
$$+ A_m \cdot (-\lambda)^{n-m} + \cdots + A = 0,$$

*) Da wir in dieser Nr. von der Voraussetzung (19) keinerlei Ge-

wo A_m die Summe der Hauptunterdeterminanten $n - m^{\text{ter}}$ Ordnung der Determinante A bedeutet.

Die wesentlichste Eigenschaft der Fundamentalgleichung besteht in dem Satze, dass sie ungeändert bleibt, wenn die Form F_a durch zwei contragrediente Substitutionen

$$(46) \qquad \begin{cases} x_\alpha = \gamma_{\alpha 1} x_1' + \gamma_{\alpha 2} x_2' + \cdots + \gamma_{\alpha n} x_n' \\ y_\alpha = q_{\alpha 1} y_1' + q_{\alpha 2} y_2' + \cdots + q_{\alpha n} y_n' \\ \qquad (\alpha = 1, 2, \cdots n) \end{cases}$$

in eine andere F_b transformirt wird. Setzt man dann

$$B(\lambda) = \begin{vmatrix} b_{11} - \lambda, & b_{12} & \cdots & b_{1n} \\ b_{21}, & b_{22} - \lambda & \cdots & b_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{n1}, & b_{n2} & \cdots & b_{nn} - \lambda \end{vmatrix},$$

so behauptet der Satz die Gleichheit

$$(47) \qquad B(\lambda) = A(\lambda).$$

Für diesen wichtigen Satz ist eine ganze Reihe von Beweisen gegeben worden*). Einer der einfachsten ist derjenige, welchen Hamburger (Journ. für Math. 76 S. 115) gegeben hat. Durch die Substitutionen (46) geht F_a in eine Form

$$F_b = \sum_{\gamma, \delta} b_{\gamma\delta}\, x_\gamma'\, y_\delta'$$

über, deren Coefficienten durch die $n \cdot n$ Gleichungen

$$b_{i\varkappa} = \sum_{\alpha, \beta} \gamma_{\alpha i}\, a_{\alpha\beta}\, q_{\beta\varkappa}$$

oder durch die allgemeine Beziehung

$$(48) \qquad b = q^{-1} \cdot a \cdot q$$

aus welcher die andere

$$(48\text{a}) \qquad q \cdot b = a \cdot q$$

---

brauch machen werden, gelten die darin enthaltenen Sätze auch für nichtsymmetrische Systeme oder Formen.

*) S. u. a. die Beweise von Fuchs (Journ. f. Math. 66 S. 132), Christoffel (ebendas. 68 S. 270), Siacci (Annali di Matem. ser. 2 tom. 4 p. 296), sowie den sich mehr an die hier gewählte Darstellung anschliessenden Beweis von Rosanes (J. f. Math. 80 S. 54).

hervorgeht, mit den Coefficienten von F_a verbunden sind. Nach dem Multiplikationssatze für Determinanten bilden wir die Produkte

$$A(\lambda)\cdot Q = | a_{\alpha 1}q_{1\beta} + \cdots + a_{\alpha n}q_{n\beta} - \lambda\cdot q_{\alpha\beta} |$$
$$Q\cdot B(\lambda) = | q_{\alpha 1}b_{1\beta} + \cdots + q_{\alpha n}b_{n\beta} - \lambda\cdot q_{\alpha\beta} |;$$

der Relation (48a) zufolge ergeben sie sich einander gleich, also

$$A(\lambda)\cdot Q = Q\cdot B(\lambda)$$

d. i. die Gleichheit (47). — Nennt man zwei Zahlensysteme a, b, welche durch die Relation

$$b = q^{-1}\cdot a\cdot q$$

mit einander verbunden sind, *ähnlich*, so lässt die erwiesene Eigenschaft der Fundamentalgleichung sich kurz so fassen: Zwei ähnliche Zahlensysteme (oder Formen) haben dieselbe Fundamentalgleichung.

So gefasst, ist der Satz nur ein Bestandtheil eines umfassenderen andern. In der That, aus (48) ergiebt sich auch diese Gleichung

$$e\lambda - b = q^{-1}\cdot(e\lambda - a)\cdot q,$$

der gemäss die Systeme $e\lambda - a$, $e\lambda - b$ in dem allgemeinen Sinne der Aequivalenz, den wir in nr. 2 behandelten, einander äquivalent sind; und umgekehrt, wenn dies der Fall ist, also eine Gleichung stattfindet:

$$e\lambda - b = p\cdot(e\lambda - a)\cdot q,$$

in welcher die Determinanten der Systeme p, q von Null verschieden sind, so folgen diese beiden:

$$e = p\cdot q,\quad b = p\cdot a\cdot q$$

also

$$b = q^{-1}\cdot a\cdot q$$

und die Systeme a, b sind ähnlich. Aehnliche Systeme a, b können mithin auch als solche definirt werden, für welche die Systeme $e\lambda - a$, $e\lambda - b$ einander äquivalent sind; und daraus folgt mittels des Weierstrass'schen Satzes sogleich das Resultat:

Damit zwei Systeme a, b (oder Formen F_a, F_b) ähnlich sind, ist nothwendig und hinreichend, dass die

Systeme $e\lambda - a$, $e\lambda - b$ dieselben Elementartheiler haben.

Insbesondere müssen also die Determinanten der letzteren Systeme d. i. die Fundamentalgleichungen der Systeme (oder Formen) a, b einander identisch sein.

Setzt man die Linearform

$$a_{\alpha 1} y_1 + a_{\alpha 2} y_2 + \cdots + a_{\alpha n} y_n - \lambda \cdot y_\alpha = A_\alpha$$
$$(\alpha = 1, 2, \cdots n)$$

und führt durch die unimodulare Substitution

$$A_\alpha' = p_{\alpha 1} A_1 + p_{\alpha 2} A_2 + \cdots + p_{\alpha n} A_n$$
$$(\alpha = 1, 2, \cdots n)$$

statt der Linearformen A_α ebenso viel andere A_α' ein, so sind die Gleichungen (44) oder

$$A_\alpha = 0$$
$$(\alpha = 1, 2, \cdots n)$$

mit den Gleichungen

$$A_\alpha' = 0$$
$$(\alpha = 1, 2, \cdots n)$$

zugleich möglich oder unmöglich. Die Bedingung für die Möglichkeit der letzteren aber ist die Gleichheit

$$(49) \qquad | a'_{\alpha\beta} - \lambda \cdot p_{\alpha\beta} | = 0,$$

in welcher

$$a'_{\alpha\beta} = p_{\alpha 1} a_{1\beta} + p_{\alpha 2} a_{2\beta} + \cdots + p_{\alpha n} a_{n\beta}$$

ist, und folglich muss diese dieselben Wurzeln haben, wie die Gleichung (45). Dem Bewiesenen zufolge muss aber ferner, wenn nun in der Form

$$F_a = \sum_\alpha A_\alpha x_\alpha$$

die Substitutionen (46) ausgeführt werden und dadurch F_a in

$$F_b = \sum_\alpha B_\alpha x_\alpha'$$

verwandelt wird, und wenn darauf durch die unimodulare Substitution

$$B_\alpha' = r_{\alpha 1} B_1 + r_{\alpha 2} B_2 + \cdots + r_{\alpha n} B_n$$
$$(\alpha = 1, 2, \cdots n)$$

statt der n Linearformen B_α ebenso viel andere B_α' eingeführt

werden, die Bedingung für die Möglichkeit der Gleichungen

$$B_\alpha' = 0$$
$$(\alpha = 1, 2, \cdots n)$$

mit den Coefficienten $b'_{\alpha\beta}$, nämlich die Gleichheit

$$| b'_{\alpha\beta} - \lambda \cdot r_{\alpha\beta} | = 0,$$

mit der Gleichung (49) gleichbedeutend sein. Die beiden Determinanten

$$| a'_{\alpha\beta} - \lambda \cdot p_{\alpha\beta} |, \quad | b'_{\alpha\beta} - \lambda \cdot r_{\alpha\beta} |$$

können sich demnach nur um einen constanten Faktor von einander unterscheiden.

6. Ist

$$f(x_i) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha x_\beta \tag{38}$$

eine quadratische Form, also

$$a_{\alpha\beta} = a_{\beta\alpha}, \tag{19}$$

so ist ihre Determinante

$$A = | a_{\alpha\beta} |$$

eine symmetrische, und folglich ergeben sich sogleich auch folgende Gleichheiten:

$$A_{\alpha\beta} = A_{\beta\alpha} \tag{50}$$

für die adjungirten Elemente und allgemeiner

$$A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} = A^{(m)}_{\varrho\sigma\tau\cdots,\,\alpha\beta\gamma\cdots}. \tag{51}$$

Dieser Gleichheit entsprechend ist der Ausdruck

$$f^{(m)}(x_{hi\varkappa\cdots}) = \sum A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \cdot x_{\alpha\beta\gamma\cdots} \cdot x_{\varrho\sigma\tau\cdots}, \tag{52}$$

wenn man darin die Summation auf alle verschiedenen (geordneten) Combinationen der Reihe $1, 2, \cdots n$ zu je m Zahlen $\alpha\beta\gamma\cdots$ einer- und zu je m Zahlen $\varrho\sigma\tau\cdots$ andererseits erstreckt, ebenfalls eine quadratische Form und zwar von

$$\mu = \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdot 3\cdots m}$$

Unbestimmten. Die Anzahl der so definirten zu einer gegebenen quadratischen Form $f(x_i)$ mit n Veränderlichen gehörigen Formen ist n; die erste von ihnen, $f^{(1)}$, ist offenbar identisch mit der Form $f(x_i)$ selbst, während die letzte, $f^{(n)}$,

sich auf $A \cdot x^2$ reducirt und von uns nicht weiter beachtet werden wird. Bezeichnet man für $m = n - 1$ mit u den nicht in der Combination der $n - 1$ Zahlen $\alpha\beta\gamma\cdots$ vorhandenen Index der Reihe $1, 2, \cdots n$, ebenso mit v den in der Combination $\varrho\sigma\tau\cdots$ fehlenden Index dieser Reihe, so ist offenbar

$$A^{(n-1)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} = (-1)^{u+v} \cdot A_{uv},$$

und wenn dann

$$x_{\alpha\beta\gamma\cdots} = (-1)^u x_u', \quad x_{\varrho\sigma\tau\cdots} = (-1)^v x_v'$$

gesetzt wird, ergiebt sich folglich

$$f^{(n-1)}(x_{hi\varkappa\cdots}) = \sum_{u,v} A_{uv} \,.\, x_u' x_v' = F(x_i')$$

d. h. die vorletzte der n Formen (52) ist bei passender Bezeichnung der Veränderlichen identisch mit einer quadratischen Form F, deren Coefficienten die adjungirten Elemente zu den Coefficienten der Form $f(x_i)$ sind, und welche daher — nach dem Vorgange von Gauss — die Adjungirte der Form $f(x_i)$ genannt werden soll. In analogem Verhältnisse, wie $f(x_i)$ zu ihrer Adjungirten, stehen zu einander die Formen $f^{(m)}$ und $f^{(n-m)}$, insofern die Coefficienten der einen (bei geeigneter Bezeichnung der Veränderlichen) zu den entsprechenden Coefficienten der anderen bezüglich der Determinante A adjungirte Unterdeterminanten sind.

Smith ist wohl der erste, welcher diese Formen (52) in der arithmetischen Theorie der quadratischen Formen verwendet hat*); er nennt sie nach englischer Ausdrucksweise die Concomitanten von $f(x_i)$, in einer späteren Arbeit**) die zu $f(x_i)$ Adjungirten der Ordnung $1, 2, \cdots n - 1$. Unabhängig von ihm hat der Verfasser sie benutzt in seiner Abhandlung „Untersuchungen über quadratische Formen" im Journ. f. Math. 76 S. 332, später Darboux in seinem Mémoire sur la théorie algébrique des formes quadratiques, Liouv. Journ.

*) Smith, On the Orders and Genera of Quadratic Forms containing more than three Indeterminates, in den Proceedings of the Royal Society of London vol. 13.

**) Smith, Mémoire sur la représentation des nombres par des sommes de cinq carrés, in Mém. prés. p. div. Savants Etrangers t. 29.

des Math. ser. 2 t. 19 p. 347. Wir wollen sie hier mit einem deutschen Namen als Begleitformen von $f(x_i)$ bezeichnen. Bei ternären Formen existirt von ihnen nur die erste, die Form $f(x_i)$ selbst, sowie die letzte, ihre Adjungirte, die Zwischenformen fallen aus, und so hatten wir dort noch keinen Anlass, von ihnen zu handeln.

Ebenso wie zur Form $f(x_i)$ gehören auch zu ihrer Adjungirten $n-1$ Begleitformen, doch sind diese nicht wesentlich von den bisherigen verschieden. Denn nach den Formeln (15) des ersten Capitels ist die Form

$$(53)\qquad F^{(m)}(x_{hi\varkappa\cdots}) = \sum \mathsf{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots}\cdot x_{\alpha\beta\gamma\cdots}\cdot x_{\varrho\sigma\tau\cdots}$$

identisch mit

$$A^{m-1}\cdot\sum \overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots}\cdot x_{\alpha\beta\gamma\cdots}\cdot x_{\varrho\sigma\tau\cdots}.$$

Sind nun $\alpha'\beta'\cdots$ diejenigen Indices der Reihe $1, 2, \cdots n$, welche übrig bleiben, wenn aus derselben $\alpha\beta\gamma\cdots$ ausgeschieden werden, und ebenso $\varrho'\sigma'\cdots$ diejenigen, welche nach Ausscheidung von $\varrho\sigma\tau\cdots$ erübrigen, so ist nach (12) des ersten Capitels

$$\overline{A}^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} = (-1)^{\alpha+\beta+\cdots+\varrho+\sigma+\cdots}\cdot A^{(n-m)}_{\alpha'\beta'\cdots,\,\varrho'\sigma'\cdots};$$

werden demnach

$$(-1)^{\alpha+\beta+\gamma+\cdots}\cdot x_{\alpha\beta\gamma\cdots} = x'_{\alpha'\beta'\cdots},$$
$$(-1)^{\varrho+\sigma+\tau+\cdots}\cdot x_{\varrho\sigma\tau\cdots} = x'_{\varrho'\sigma'\cdots}$$

gesetzt, so geht $F^{(m)}$ über in die Form

$$F^{(m)}(x_{hi\varkappa\cdots}) = A^{m-1}\cdot\sum A^{(n-m)}_{\alpha'\beta'\cdots,\,\varrho'\sigma'\cdots}\cdot x'_{\alpha'\beta'\cdots}\cdot x'_{\varrho'\sigma'\cdots}$$

d. h. es ist allgemein

$$(54)\qquad F^{(m)}(x_{hi\varkappa\cdots}) = A^{m-1}\cdot f^{(n-m)}(x'_{h'i'\cdots}).$$

Durch Differenzirung der Gleichung (52) findet man, wenn zur Abkürzung

$$(55)\qquad X_{\alpha\beta\gamma\cdots} = \frac{1}{2}\,\frac{\partial f^{(m)}}{\partial x_{\alpha\beta\gamma\cdots}}$$

gesetzt wird, das System der μ Gleichungen:

$$(56)\qquad X_{\alpha\beta\gamma\cdots} = \sum_{\varrho\sigma\tau\cdots} A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots}\cdot x_{\varrho\sigma\tau\cdots},$$

(für die μ Combinationen $\alpha\beta\gamma\cdots$)

deren Auflösung gelingt, wenn man sich der Beziehungen (13) des ersten Capitels bedient, welche hier wegen (51) so geschrieben werden können:

$$A = \sum_{\alpha\beta\gamma\cdots} A^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots} \cdot \overline{A}^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots}$$

$$0 = \sum_{\alpha\beta\gamma\cdots} A^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots} \cdot \overline{A}^{(m)}_{\alpha\beta\gamma\cdots, \varrho\sigma\tau\cdots}.$$

Werden nämlich die Gleichungen (56) der Reihe nach mit

$$\overline{A}^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots}$$

multiplicirt und dann bezüglich aller Combinationen $\alpha\beta\gamma\cdots$ addirt, so gewinnt man die Umkehrung derselben in folgender Gestalt:

$$A \cdot x_{rst\cdots} = \sum_{\alpha\beta\gamma\cdots} \overline{A}^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots} \cdot X_{\alpha\beta\gamma\cdots}$$

oder besser, indem man

$$A^m \cdot x_{rst\cdots} = \mathfrak{x}_{rst\cdots} \tag{57}$$

setzt, nach Formel (15) des ersten Capitels

$$\mathfrak{x}_{rst\cdots} = \sum \mathsf{A}^{(m)}_{\alpha\beta\gamma\cdots, rst\cdots} \cdot X_{\alpha\beta\gamma\cdots}. \tag{58}$$

(für die μ Combinationen $rst\cdots$)

Hieraus folgt zunächst, wenn man mit

$$\frac{1}{2}\frac{\partial f^{(m)}}{\partial x_{rst\cdots}} = X_{rst\cdots}$$

multiplicirt und dann über die verschiedenen Combinationen $rst\cdots$ summirt, nach dem Euler'schen Satze die folgende Gleichung:

$$A^m \cdot f^{(m)}(x_{hi\varkappa\cdots}) = F^{(m)}(X_{hi\varkappa\cdots}). \tag{59}$$

Nun stehen aber die Werthe von $\mathfrak{x}_{rst\cdots}$ oder die Gleichungen (58) zur Form $F^{(m)}$ offenbar in genau derselben Beziehung, wie die Werthe von $X_{\alpha\beta\gamma\cdots}$ oder die Gleichungen (56) zur Form $f^{(m)}$. Daraus folgt einerseits, dass

$$\left| A^{(m)}_{\alpha\beta\gamma\cdots, \varrho\sigma\tau\cdots} \right| \text{ und } \left| \mathsf{A}^{(m)}_{\alpha\beta\gamma\cdots, \varrho\sigma\tau\cdots} \right|$$

die Determinanten der Formen $f^{(m)}$ und $F^{(m)}$ resp. sind, und zwischen ihnen der Formel (14) des ersten Ca-

pitels zufolge die Beziehung:

$$(60)\qquad \left| A^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} \right| \cdot \left| \mathsf{A}^{(m)}_{\alpha\beta\gamma\cdots,\varrho\sigma\tau\cdots} \right| = A^{m\mu}.$$

Andererseits ergiebt sich analog der Gleichung (59) die folgende:

$$\mathsf{A}^m \cdot F^{(m)}(X_{hi\varkappa}\ldots) = \varphi^{(m)}(\xi_{hi\varkappa}\ldots),$$

wenn unter $\varphi^{(m)}$ diejenige quadratische Form verstanden wird, die aus $F^{(m)}$ in gleicher Weise entsteht, wie diese aus $f^{(m)}$. Verbindet man vorstehende Gleichung nun mit den Gleichungen (57) und (59) und achtet auf den Werth von A sowohl, wie auf die Homogeneïtät der Formen, so erhält man folgendes Resultat:

$$(61)\qquad A^{m(n-2)} \cdot f^{(m)}(x_{hi\varkappa}\ldots) = \varphi^{(m)}(x_{hi\varkappa}\ldots)$$

d. h. man erhält die Form $\varphi^{(m)}$ einfach dadurch, dass man alle Coefficienten von $f^{(m)}$ mit $A^{m(n-2)}$ multiplicirt.

Wir heben aus den allgemeinen Sätzen über die Begleitformen, zu denen wir gelangt sind, ausdrücklich diejenigen besonderen hervor, welche für die Adjungirte gelten. Für $m = 1$ findet sich nämlich:

Sind die Grössen X_i mit den x_i vermittelst der Gleichungen (40) oder (41) verbunden, so wird die Gleichung

$$(62)\qquad F(X_i) = A \cdot f(x_i)$$

identisch erfüllt.

Die Determinante der adjungirten Form F ist gleich der $n - 1^{\text{ten}}$ Potenz von der Determinante der ursprünglichen Form f.

Man erhält die Adjungirte von der adjungirten Form aus der ursprünglichen Form, wenn man die Coefficienten der letzteren mit der $n - 2^{\text{ten}}$ Potenz ihrer Determinante multiplicirt.

7. Wenn die quadratische Form

$$(38)\qquad f(x_i) = \sum_{\alpha,\beta} a_{\alpha\beta}\, x_\alpha\, x_\beta$$

durch die Substitution (26) in eine andere quadratische Form

$$g(x_i') = \sum_{\alpha,\beta} b_{\alpha\beta}\, x_\alpha'\, x_\beta'$$

übergeht, so werden die Coefficienten dieser neuen Form durch die der ursprünglichen mittels der allgemeinen Formel (22) oder (23):

$$b_{\gamma\delta} = \sum_{\alpha,\beta} a_{\alpha\beta}\, q_{\alpha\gamma}\, q_{\beta\delta}$$

geliefert. Nach (38) ist

$$(63)\qquad f(q_{\iota x}) = \sum_{\alpha,\beta} a_{\alpha\beta}\, q_{\alpha x}\, q_{\beta x};$$

setzt man daher zur Abkürzung

$$(64)\qquad \frac{1}{2}\,\frac{\partial f(q_{ix})}{\partial q_{\alpha x}} = f^{\alpha}(q_{ix}),$$

so wird

$$(65)\qquad f^{\alpha}(q_{ix}) = \sum_{\beta} a_{\alpha\beta}\, q_{\beta x}$$

und folglich

$$(66)\qquad b_{\gamma\delta} = \sum_{\alpha} q_{\alpha\gamma}\cdot f^{\alpha}(q_{i\delta}).$$

Diese allgemeine Formel für die Coefficienten der transformirten Form steht für die folgenden

$$n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$$

besonderen, die wir die Transformationsrelationen nennen wollen:

$$(67)\qquad \begin{cases} b_{\gamma\gamma} = q_{1\gamma} f^{1}(q_{i\gamma}) + \cdots + q_{n\gamma} f^{n}(q_{i\gamma}) = f(q_{i\gamma}) \\ \qquad\qquad (\gamma = 1, 2, \cdots n) \\ b_{\gamma\delta} = q_{1\gamma} f^{1}(q_{i\delta}) + \cdots + q_{n\gamma} f^{n}(q_{i\delta}) \\ \quad\;\; = q_{1\delta} f^{1}(q_{i\gamma}) + \cdots + q_{n\delta} f^{n}(q_{i\gamma}) = b_{\delta\gamma}. \\ \qquad\qquad (\gamma \gtrless \delta) \end{cases}$$

Der Formel (65) zufolge ist das System

$$(68)\qquad \begin{cases} f^{1}(q_{i1}), & f^{1}(q_{i2}), & \cdots & f^{1}(q_{in}) \\ \cdot & \cdot & \cdot & \cdot \\ f^{n}(q_{i1}), & f^{n}(q_{i2}), & \cdots & f^{n}(q_{in}) \end{cases}$$

aus den beiden Systemen a und q zusammengesetzt, gleicherweise ist das System b aus dem System q' und dem eben bezeichneten zusammengesetzt. Hieraus, oder auch aus (22) unmittelbar, folgt zunächst für die Determinanten der Systeme die Beziehung

$$(69)\qquad B = Q \cdot A \cdot Q = A \cdot Q^2;$$

die Determinante der transformirten Form ist gleich derjenigen der ursprünglichen Form, multiplicirt in das Quadrat des Substitutionsmodulus.

Wir nennen die Formen $f(x_i)$ und $g(x_i')$ einander äquivalent, wenn die eine in die andere durch eine Substitution (26) übergeht, deren Modulus gleich ± 1 ist. Die Aequivalenz wird als eine eigentliche bezeichnet, wenn der Modulus der positiven Einheit, als uneigentliche, wenn er der negativen Einheit gleich ist. Formen mit einer ungeraden Anzahl von Veränderlichen sind, wenn sie einander äquivalent sind, es stets zugleich eigentlich und uneigentlich, denn, werden alle Veränderlichen der einen Form entgegengesetzt genommen, so bleibt einerseits die Form unverändert, andererseits aber verändert der Modulus der Substitution sein Vorzeichen. Bei Formen mit einer geraden Anzahl von Veränderlichen hätte man dagegen zwischen eigentlicher und uneigentlicher Aequivalenz zu unterscheiden, doch beschränken wir uns hier ausschliesslich auf die Betrachtung der eigentlichen Aequivalenz.

Aequivalente Formen haben gleiche Determinanten.

Ferner aber folgt aus (17) des ersten Capitels, wenn darin unter C die Determinante des Systems (68) verstanden wird, die Beziehung

$$C^{(m)}_{\alpha\beta\gamma\cdots,\,rst\cdots} = \sum_{\varrho\sigma\tau\cdots} A^{(m)}_{\alpha\beta\gamma\cdots,\,\varrho\sigma\tau\cdots} \cdot Q^{(m)}_{\varrho\sigma\tau\cdots,\,rst\cdots}$$

und, wenn dieselbe Formel auf die Determinante B des Systems b angewandt wird, in gleicher Weise

$$B^{(m)}_{hi\varkappa\cdots,\,rst\cdots} = \sum_{\alpha\beta\gamma\cdots} Q^{(m)}_{\alpha\beta\gamma\cdots,\,hi\varkappa\cdots} \cdot C^{(m)}_{\alpha\beta\gamma\cdots,\,rst\cdots}.$$

Der ersteren dieser beiden Gleichungen kann man mit Rücksicht auf (52) die Gestalt geben:

$$C^{(m)}_{\alpha\beta\gamma\cdots,\,rst\cdots} = \frac{1}{2}\,\frac{\partial f^{(m)}\left(Q^{(m)}_{\varrho\sigma\tau\cdots,\,rst\cdots}\right)}{\partial Q^{(m)}_{\alpha\beta\gamma\cdots,\,rst\cdots}},$$

wodurch dann die letztere der Gleichungen in die Gestalt

(70) $$B^{(m)}_{hi\varkappa\cdots,rst\cdots} = \sum_{\alpha\beta\gamma\cdots} Q^{(m)}_{\alpha\beta\gamma\cdots,hi\varkappa\cdots} \cdot \frac{1}{2}\,\frac{\partial f^{(m)}(Q^{(m)}_{\varrho\sigma\tau\cdots,rst\cdots})}{\partial Q^{(m)}_{\alpha\beta\gamma\cdots,rst\cdots}}$$

übergeht und in Analogie mit der Formel (66) folgenden Satz ausspricht:

Geht $f(x_i)$ durch die Substitution (26) über in $g(x_i')$, so verwandelt sich die m^{te} Begleitform von $f(x_i)$ durch die Substitution

(71) $$\xi_{hi\varkappa\cdots} = \sum_{\varrho\sigma\tau\cdots} Q^{(m)}_{hi\varkappa\cdots,\varrho\sigma\tau\cdots} \cdot \xi'_{\varrho\sigma\tau\cdots}$$

(für die μ Combinationen $hi\varkappa\cdots$)

in die m^{te} Begleitform von $g(x_i')$.

Setzt man insbesondere $m = n - 1$ und nennt $Q_{\alpha\beta}$ das zu $q_{\alpha\beta}$ adjungirte Element der Determinante Q, so erhält man den Zusatz: Geht $f(x_i)$ durch die Substitution (26) in $g(x_i')$ über, so verwandelt sich die Adjungirte von $f(x_i)$ durch die Substitution

(72) $$\xi_i = Q_{i1}\xi_1' + Q_{i2}\xi_2' + \cdots + Q_{in}\xi_n'$$
$$(i = 1, 2, \cdots n)$$

in die Adjungirte von $g(x_i')$*). Dies Resultat bestätigt man leicht mittels der Formel (62). Denn, nennt man $G(X_i')$ die Adjungirte von $g(x_i')$, so wird dieser Formel zufolge

(73) $$G(X_i') = B \cdot g(x_i')$$

sein, wenn man

$$X_\gamma' = \frac{1}{2}\,\frac{\partial g(x_i')}{\partial x_\gamma'} = b_{\gamma 1}x_1' + b_{\gamma 2}x_2' + \cdots + b_{\gamma n}x_n'$$
$$(\gamma = 1, 2, \cdots n)$$

setzt. Geht aber $f(x_i)$ durch die Substitution (26) in $g(x_i')$ über, so folgt wegen (66)

$$X_\gamma' = \sum_{\alpha,\delta} q_{\alpha\gamma} f^\alpha(q_{i\delta})x_\delta' = \sum_{\alpha,\delta} q_{\alpha\delta}x_\delta' \cdot f^\alpha(q_{i\gamma})$$

d. h. gleich

$$\sum_\alpha x_\alpha f^\alpha(q_{i\gamma}) = \sum_\alpha q_{\alpha\gamma} f^\alpha(x_i)$$

---

*) Die Adjungirte von $f(x_i)$ heisst deshalb auch die Contravariante dieser Form.

oder

$$(26a)\qquad X_\gamma' = q_{1\gamma}X_1 + q_{2\gamma}X_2 + \cdots + q_{n\gamma}X_n \quad (\gamma = 1, 2, \cdots n)$$

also auch umgekehrt

$$Q \cdot X_i = Q_{i1}X_1' + Q_{i2}X_2' + \cdots + Q_{in}X_n'. \quad (i = 1, 2, \cdots n)$$

Durch diese Substitution muss also

$$\frac{F(X_i)}{A} \text{ in } \frac{G(X_i')}{B}$$

und folglich, da $B = AQ^2$ ist, durch die Substitution (72)

$$F(\xi_i) \text{ in } G(\xi_i')$$

sich verwandeln.

Ist $Q = 1$, so hat nach (14a) des ersten Capitels auch der Modulus der Substitution (71) die Einheit zum Werthe. Man findet hiernach noch den besonderen Satz: Sind die Formen $f(x_i)$ und $g(x_i')$ einander äquivalent, so sind es auch ihre Begleitformen je derselben Ordnung.

8. Wir müssen hauptsächlich diejenigen Transformationen einer quadratischen Form hervorheben, welche sie in sich selbst verwandeln. Ist

$$(26)\qquad x_i = q_{i1}x_1' + q_{i2}x_2' + \cdots + q_{in}x_n' \quad (i = 1, 2, \cdots n)$$

eine Transformation der Form $f(x_i)$ in sich selbst, so verwandelt zugleich die Substitution (71) die m^{te} Begleitform $f^{(m)}$ in sich selbst. Dem entsprechend gehen die Formeln (67) und (70) in folgende Gestalt über, in welcher zur Abkürzung

$$(74)\qquad \frac{1}{2}\frac{\partial f(q_{i\gamma})}{\partial q_{\delta\gamma}} = f^{\delta}(q_{i\gamma}) = f_{\delta\gamma}$$

$$(75)\qquad \frac{1}{2}\frac{\partial f^{(m)}(Q^{(m)}_{\varrho\sigma\tau\cdots,rst\cdots})}{\partial Q^{(m)}_{\alpha\beta\gamma\cdots,rst\cdots}} = f^{(m)}_{\alpha\beta\gamma\cdots}(Q^{(m)}_{\varrho\sigma\tau\cdots,rst\cdots})$$

gesetzt worden ist:

$$(76)\qquad a_{\gamma\delta} = q_{1\delta}\cdot f_{1\gamma} + q_{2\delta}\cdot f_{2\gamma} + \cdots + q_{n\delta}\cdot f_{n\gamma} \quad (\gamma, \delta = 1, 2, \cdots n)$$

$$(77)\qquad A^{(m)}_{hix\cdots,rst\cdots} = \sum_{\alpha\beta\gamma} Q^{(m)}_{\alpha\beta\gamma\cdots,hix\cdots}\cdot f^{(m)}_{\alpha\beta\gamma\cdots}(Q^{(m)}_{\varrho\sigma\tau\cdots,rst\cdots}).$$

Insbesondere aber stellen dann die Gleichungen (72), folglich auch ihre Auflösung

(78) $$\xi_i' = q_{1i}\xi_1 + q_{2i}\xi_2 + \cdots + q_{ni}\xi_n \quad (i = 1, 2, \cdots n)$$

eine Transformation der **Adjungirten** in sich selbst vor. Man erhält somit zunächst die Formeln

(79) $$A_{\gamma\delta} = q_{\delta 1}F_{1\gamma} + q_{\delta 2}F_{2\gamma} + \cdots + q_{\delta n}F_{n\gamma}, \quad (\gamma, \delta = 1, 2, \cdots n)$$

wo zur Abkürzung

(80) $$\frac{1}{2}\,\frac{\partial F(q_{\gamma i})}{\partial q_{\gamma\delta}} = F^\delta(q_{\gamma i}) = F_{\delta\gamma}$$

gesetzt ist; zugleich geht aber die m^{te} Begleitform $F^{(m)}$ der Adjungirten durch die Substitution

(81) $$\xi_{hi\varkappa\cdots} = \sum_{\varrho\sigma\tau\cdots} Q^{(m)}_{\varrho\sigma\tau\cdots,\,hi\varkappa\cdots}\cdot\xi'_{\varrho\sigma\tau\cdots}$$

in sich selbst über und man findet demnach noch die mit (77) analoge Gleichung:

(82) $$\mathsf{A}^{(m)}_{hi\varkappa\cdots,\,rst\cdots} = \sum_{\alpha\beta\gamma\cdots} Q^{(m)}_{hi\varkappa\cdots,\,\alpha\beta\gamma\cdots}\cdot F^{(m)}_{\alpha\beta\gamma\cdots}(Q^{(m)}_{rst\cdots,\,\varrho\sigma\tau\cdots}).$$

Nun bezeichne $\mathfrak{Q}$ die Determinante der Gleichungen (72); nach Gleichung (15) des ersten Capitels ist dann, da $Q = 1$ ist

$$\mathfrak{Q}^{(m)}_{hi\varkappa\cdots,\,uvw\cdots} = \overline{Q}^{(m)}_{hi\varkappa\cdots,\,uvw\cdots}.$$

Wird demnach die vorige Gleichung links und rechts mit diesen gleichen Grössen multiplicirt, und dann über alle Combinationen $hi\varkappa\cdots$ summirt, so findet sich wegen (50) und mit Rücksicht darauf, dass nach (13) des ersten Capitels

$$\sum_{hi\varkappa\cdots} Q^{(m)}_{hi\varkappa\cdots,\,\alpha\beta\gamma\cdots}\cdot\overline{Q}^{(m)}_{hi\varkappa\cdots,\,uvw\cdots}$$

gleich Q oder gleich Null ist, jenachdem die Combinationen $\alpha\beta\gamma\cdots$, $uvw\cdots$ dieselben sind oder nicht, folgende **bemerkenswerthe Beziehung**:

(83) $$F^{(m)}_{rst\cdots}(\mathfrak{Q}^{(m)}_{\varrho\sigma\tau\cdots,\,uvw\cdots}) = F^{(m)}_{uvw\cdots}(Q^{(m)}_{rst\cdots,\,\varrho\sigma\tau\cdots}).$$

Wird jedoch diese nun weiter mit

$$A^{(m)}_{rst\cdots,\,uvw\cdots} = A^{(m)}_{uvw\cdots,\,rst\cdots}$$

beiderseits multiplicirt und dann über alle Combinationen $rst\cdots$ sowohl wie $uvw\cdots$ summirt, so entsteht die Gleichung

$$
(84)\qquad \begin{cases} \sum A^{(m)}_{rst\cdots,uvw\cdots}\cdot F^{(m)}_{rst\cdots}(\mathfrak{Q}^{(m)}_{\varrho\sigma\tau\cdots,uvw\cdots}) \\ =\sum A^{(m)}_{uvw\cdots,rst\cdots}\cdot F^{(m)}_{uvw\cdots}(Q^{(m)}_{rst\cdots,\varrho\sigma\tau\cdots}), \end{cases}
$$

in der wir links die Summation nach $rst\cdots$, rechts die nach $uvw\cdots$ zuerst ausführen wollen. Da dann links

$$
\sum A^{(m)}_{rst\cdots,uvw\cdots}\cdot \mathsf{A}^{(m)}_{rst\cdots,\varrho\sigma\tau\cdots}\cdot \mathfrak{Q}^{(m)}_{\varrho\sigma\tau\cdots,uvw\cdots},
$$

bezogen auf alle Combinationen $rst\cdots$ und $\varrho\sigma\tau\cdots$ zu bilden ist, so ist das Resultat dieser Summation nach den Formeln (15) und (13) des ersten Capitels

$$
A^m\cdot \mathfrak{Q}^{(m)}_{uvw\cdots,uvw\cdots},
$$

und somit wird die linke Seite der Gleichung gleich

$$
A^m\cdot \sum_{uvw\cdots} \mathfrak{Q}^{(m)}_{uvw\cdots,uvw\cdots};
$$

und da in gleicher Weise die rechte Seite gleich

$$
A^m\cdot \sum_{rst\cdots} Q^{(m)}_{rst\cdots,rst\cdots}
$$

gefunden wird, ergiebt sich endlich die wichtige Formel:

$$
(85)\qquad \sum_{rst\cdots} \mathfrak{Q}^{(m)}_{rst\cdots,rst\cdots} = \sum_{rst\cdots} Q^{(m)}_{rst\cdots,rst\cdots}.
$$

Nun stellt aber (s. 45a) die rechte Seite dieser Formel den Coefficienten von $(-\lambda)^{n-m}$ in der Fundamentalgleichung

$$
(-1)^n\,|\,e\lambda - q\,| = 0,
$$

und aus gleichem Grunde ihre linke Seite den Coefficienten von $(-\lambda)^{n-m}$ in der Fundamentalgleichung

$$
(-1)^n\,|\,e\lambda - q^{-1}\,| = 0
$$

dar, welcher wir, da $Q = 1$ ist, auch die Form

$$
(\lambda)^n\cdot|\,e\cdot\frac{1}{\lambda} - q\,| = 0
$$

geben können. Man erhält mit anderen Worten die Gleichheit

$$
(86)\qquad (-\lambda)^n\cdot|\,e\cdot\frac{1}{\lambda} - q\,| = |\,e\lambda - q\,|
$$

d. h. die Fundamentalgleichung einer Substitution, welche eine quadratische Form von nicht verschwindender Determinante (eigentlich) in sich selbst verwandelt, ist eine reciproke Gleichung. Dieser wichtige Satz ist zuerst von Cayley bemerkt worden*). Wir haben ihn hier mittels einfacher Determinantensätze unmittelbar aus den Transformationsrelationen hergeleitet. Einen anderen sehr einfachen Beweis gab Rosanes**). Geht nämlich $f(x_i)$ durch die Substitution (26) mit dem Modulus 1 in sich selbst über, so bestehen neben den Gleichungen (26) die Gleichungen (26a), wenn darin

$$X_\gamma' = \frac{1}{2}\frac{\partial f(x_i')}{\partial x_\gamma'} = a_{\gamma 1}x_1' + \cdots + a_{\gamma n}x_n'$$

gedacht wird, und sind nur als eine andere Form der ersteren anzusehen. Setzt man nun $x_i = \lambda x_i'$, so wird der letztgeschriebenen Formel zufolge $X_i' = \frac{1}{\lambda}\cdot X_i$. Demnach lässt sich die Bedingung für das Bestehen der Gleichungen (26) unter der Voraussetzung $x_i = \lambda x_i'$, nämlich die Fundamentalgleichung

$$|\, e\lambda - q \,| = 0, \tag{87}$$

auch folgendermassen schreiben:

$$|\, e\cdot\frac{1}{\lambda} - q' \,| = 0,$$

eine Gleichung, welche bei Vertauschung der Zeilen mit den Spalten in der Determinante zur Linken auch durch diese andere:

$$|\, e\cdot\frac{1}{\lambda} - q \,| = 0 \tag{88}$$

ersetzt werden darf. Die Gleichungen (87) und (88) haben mithin die nämlichen Wurzeln.

9. Dieser Satz spricht eine Eigenschaft jeder Substitution, welche eine quadratische Form von nicht verschwindender Determinante in sich selbst transformirt, ganz unabhängig von der Form aus, welche sie zu transformiren vermag, und regt

*) Cayley, sur la transformation d'une fonction quadratique en elle-même par des substitutions linéaires, Journ. f. Math. 50 S. 288—299.

**) Journ. f. Math. 80 S. 62.

die Frage an, welches die nothwendige und hinreichende Bedingung sei, damit eine Substitution sich eigne, eine quadratische Form von nicht verschwindender Determinante in sich selbst zu transformiren. Eine erste dahingehende Bemerkung verdankt man Rosanes*). Ist a ein Zahlensystem von nicht verschwindender Determinante (das übrigens nicht symmetrisch zu sein braucht), so betrachte man die Gleichungen

$$(89)\qquad \left\{\begin{aligned} & a_{\alpha 1} x_1 + a_{\alpha 2} x_2 + \cdots + a_{\alpha n} x_n \\ & = a_{1\alpha} x_1' + a_{2\alpha} x_2' + \cdots + a_{n\alpha} x_n'; \\ & \qquad (\alpha = 1, 2, \cdots n) \end{aligned}\right.$$

ihren eigenthümlichen Aufbau zu kennzeichnen, nennt Rosanes ihr System ein antisymmetrisches. Werden diese Gleichungen beiderseits einmal mit x_α, das andere Mal mit x_α' multiplicirt und jedesmal dann über $\alpha = 1, 2, \cdots n$ summirt, so entstehen die folgenden zwei Gleichungen:

$$\sum_{\alpha,\beta} a_{\alpha\beta}\, x_\alpha\, x_\beta = \sum_{\alpha,\beta} a_{\beta\alpha}\, x_\alpha\, x_\beta'$$

$$\sum_{\alpha,\beta} a_{\alpha\beta}\, x_\beta\, x_\alpha' = \sum_{\alpha,\beta} a_{\beta\alpha}\, x_\alpha'\, x_\beta',$$

deren letzte bei Vertauschung der Summationsbuchstaben auch so geschrieben werden kann:

$$\sum_{\alpha\beta} a_{\beta\alpha}\, x_\alpha\, x_\beta' = \sum_{\alpha,\beta} a_{\alpha\beta}\, x_\alpha'\, x_\beta',$$

und durch Vergleichung mit der ersteren findet sich sogleich

$$\sum_{\alpha,\beta} a_{\alpha\beta}\, x_\alpha\, x_\beta = \sum_{\alpha,\beta} a_{\alpha\beta}\, x_\alpha'\, x_\beta'.$$

Die antisymmetrische Substitution (89) transformirt also die homogene quadratische Funktion — insbesondere, wenn a symmetrisch ist, die quadratische Form —

$$(90)\qquad \sum a_{\alpha\beta}\, x_\alpha\, x_\beta$$

in sich selbst.

Allgemeiner ist zu sagen: Soll die Substitution (26) mit

*) S. a. a. O. § 2 und 3.

dem Modulus $Q=1$ die Funktion — oder, falls a symmetrisch ist, die quadratische Form — (90) in sich selbst transformiren, so muss nach (22) die Beziehung

(91) $$a = q' \cdot a \cdot q$$

erfüllt sein. Untersuchen wir also genauer, wie beschaffen q hierzu sein muss.

Man schliesst zunächst aus (91) durch Uebergang zu den conjugirten Systemen die Gleichung

$$a' = q' \cdot a' \cdot q$$

und durch Uebergang zu den reciproken Systemen die folgende:

$$a^{-1} = q^{-1} \cdot a^{-1} \cdot q'^{-1},$$

durch Verbindung der beiden aber entsteht diese dritte:

$$a^{-1} \cdot a' = q^{-1} \cdot a^{-1} \cdot q'^{-1} \cdot q' \cdot a' \cdot q = q^{-1} \cdot a^{-1} a' \cdot q$$

oder

(92) $$q \cdot u = u \cdot q,$$

wenn

(93) $$u = a^{-1} a'$$

gesetzt wird. Nun ist ersichtlich u das System der Coefficienten in der durch Auflösung der antisymmetrischen Gleichungen (89) nach den Grössen x_α erhaltenen Substitution. Heisst letztere wieder eine antisymmetrische Substitution, so lehrt die Gleichung (92) den Satz: Damit die Substitution (26) die Funktion (quadratische Form) (90) in sich selbst transformiren kann, muss q mit dem Coefficientensysteme der antisymmetrischen Substitution, welche jener Funktion (quadratischen Form) zugehört, vertauschbar sein*).

Ferner aber folgt aus (91) auch die Gleichung

(94) $$q'a(\lambda e - q) = (\lambda q' - e)a$$

oder

$$q'a(\lambda e - q) = -\lambda \cdot \left(\frac{1}{\lambda} e - q'\right) a.$$

Indem man beiderseits die Determinanten bildet wird man zunächst auf die einfachste Weise zur

*) S. Frobenius Journ. f. Math. 84 S. 36 Satz VII.

Gleichung (86):

$$|\lambda e - q| = (-\lambda)^n \cdot \left|\frac{1}{\lambda} e - q\right|$$

wieder zurückgeführt. Dieser Gleichung zufolge hat bei ungeradem n die Fundamentalgleichung

$$|\lambda e - q| = 0$$

immer die Wurzel $\lambda = 1$. Da ferner das Produkt aller ihrer Wurzeln gleich $Q = 1$, das Produkt je zweier reciproker Wurzeln der Gleichung aber ebenfalls 1 ist, muss die Anzahl der Wurzeln, welche -1 sind, immer gerade sein.

Ferner aber lehrt die Gleichung (94), dass die beiden Systeme

$$\lambda e - q, \quad \lambda q' - e$$

im Sinne der nr. 2 einander äquivalent sind. Nun sind zwei conjugirte Systeme q und q' einander stets ähnlich, denn die zugehörigen Systeme

$$\lambda e - q \text{ und } \lambda e - q'$$

haben offenbar gleiche Elementartheiler. Es giebt folglich ein System u mit nicht verschwindender Determinante, für welches

$$q' = u^{-1} \cdot q \cdot u \tag{95}$$

und folglich

$$\lambda q' - e = u^{-1}(\lambda q - e)u$$

ist. Demnach müssen auch die beiden Systeme

$$\lambda e - q \text{ und } \lambda q - e$$

einander äquivalent sein. — Erfüllt aber das System q diese nothwendige Bedingung, so giebt es auch ein System a von nicht verschwindender Determinante, für welches die Beziehung (91) besteht. In der That giebt es alsdann Systeme v, w von nicht verschwindender Determinante, so beschaffen, dass

$$v(\lambda e - q)w = \lambda q - e$$

also

$$vw = q, \quad vqw = e$$

mithin

$$v = w^{-1}q^{-1} \tag{96}$$

ist. Aus (95) folgt daher

$$q' = u^{-1} \cdot vw \cdot u$$

also

$$v = uq'u^{-1}w^{-1}$$

und wegen (96)

$$w^{-1}q^{-1} = uq'u^{-1}w^{-1}$$

oder

$$u^{-1}w^{-1} = q' \cdot u^{-1}w^{-1} \cdot q$$

und folglich ist

$$a = u^{-1}w^{-1}$$

ein System von nicht verschwindender Determinante, so beschaffen, dass die Beziehung

$$a = q' \cdot a \cdot q$$

erfüllt wird.

Dies System braucht jedoch nicht symmetrisch zu sein. Es bliebe demnach noch festzustellen, welche weitere Bedingungen q erfüllen muss, damit die Beziehung (91) für ein symmetrisches System a stattfinden kann. Diese Untersuchung ist von Frobenius (a. a. O. S. 41) geführt worden und das Resultat ist folgendes: Damit eine Substitution (26) geeignet sei, eine quadratische Form von nicht verschwindender Determinante in sich selbst zu transformiren, ist nothwendig und hinreichend, dass die Elementartheiler des Systems $\lambda e - q$ paarweise von gleichem Grade sind und für reciproke Werthe verschwinden, mit Ausnahme derer, welche für $\lambda = 1$ oder $\lambda = -1$ verschwinden und *einen ungeraden Exponenten* haben. Wir müssen uns hier damit begnügen, diesen Satz auszusprechen, und im Uebrigen den Leser auf die Abhandlung von Frobenius verweisen.

10. Nachdem auf solche Weise der allgemeine Charakter jeder Substitution gekennzeichnet worden, welche eine quadratische Form überhaupt in sich selbst zu transformiren geeignet ist, muss weiter nach dem Ausdrucke derjenigen Substitutionen gefragt werden, durch welche eine *bestimmte, gegebene* quadratische Form von nicht verschwindender Determinante in sich selbst übergeführt wird. Die Lösung dieser Aufgabe ist zuerst von Cayley

und Hermite*) versucht worden. Hermite's Methode besteht in der folgenden Ueberlegung.

Soll die Substitution (26) die quadratische Form

$$f(x_i) = \sum_{\alpha,\beta} a_{\alpha\beta} x_\alpha x_\beta$$

in sich selbst verwandeln, so findet vermöge der durch die Substitution zwischen den Variabeln x_α und x_α' ausgesprochenen Beziehung die identische Gleichung

$$(97) \qquad f(x_i) = f(x_i')$$

statt. Diese eine Gleichung oder die ihr entsprechenden $\frac{n(n+1)}{2}$ Transformationsrelationen (76) zwischen den $n \cdot n$ gesuchten Substitutionscoefficienten lassen $\frac{n(n-1)}{2}$ der letzteren unbestimmt oder gestatten nur, die Coefficienten als Funktionen von $\frac{n(n-1)}{2}$ willkürlichen Parametern zu bestimmen. Um dahin zu gelangen, setze man

$$x_\alpha + x_\alpha' = 2\xi_\alpha, \quad (\alpha = 1, 2, \cdots n)$$

wodurch die Gleichung (97) die neue Gestalt

$$f(x_i) = 4f(\xi_i) - 4\sum a_{\alpha\beta} x_\alpha \xi_\beta + f(x_i)$$

oder einfacher die Gestalt

$$\sum_\alpha (\xi_\alpha - x_\alpha) \cdot \frac{1}{2} \frac{\partial f(\xi_i)}{\partial \xi_\alpha} = 0$$

erhält. Versteht man nun unter $s_{\alpha\beta}$ für

$$\alpha, \beta = 1, 2, \cdots n$$

ein System von n^2 Zahlen, die nur der Bedingung

$$s_{\alpha\beta} + s_{\beta\alpha} = 0$$

unterworfen sind, so genügt man vorstehender Gleichung, indem man setzt:

*) S. ausser der schon oben genannten Abhandlung von Cayley seine Arbeiten: sur quelques propriétés des déterminants gauches, und recherches ultérieures sur les déterminants gauches im Journ. für Math. 32 resp. 50, und Hermite, sur la théorie des formes quadratiques, ebendas. 47 v. S. 307 an.

$$\xi_\alpha - x_\alpha = \sum_\beta s_{\alpha\beta} \cdot \frac{1}{2} \frac{\partial f(\xi_i)}{\partial \xi_\beta},$$

denn

$$\sum_{\alpha,\beta} s_{\alpha\beta} \cdot \frac{1}{4} \frac{\partial f(\xi_i)}{\partial \xi_\alpha} \frac{\partial f(\xi_i)}{\partial \xi_\beta}$$

ist Null. Demnach wird man durch Elimination der Variabeln ξ_α zwischen den beiden Systemen von Gleichungen

$$x_\alpha = \xi_\alpha - \sum_\beta \xi_\beta \cdot \frac{1}{2} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}} \qquad (\alpha = 1, 2, \cdots n) \tag{98}$$

und

$$x_\alpha' = \xi_\alpha + \sum_\beta \xi_\beta \cdot \frac{1}{2} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}} \qquad (\alpha = 1, 2, \cdots n) \tag{99}$$

ein System von n Gleichungen zwischen den x_α und x_α' erhalten, deren Coefficienten rational von den $\frac{n(n-1)}{2}$ willkürlichen Grössen $s_{\alpha\beta}$ abhängen und welche für alle Werthe dieser Grössen eine Transformation der quadratischen Form $f(x_i)$ in sich selbst ergeben.

Die Elimination der Variabeln ξ_α aber lässt sich folgendermassen bewerkstelligen:

Zunächst folgt aus (98) die Gleichung

$$\frac{1}{2} \frac{\partial f(x_i)}{\partial x_\gamma} = \frac{1}{2} \frac{\partial f(\xi_i)}{\partial \xi_\gamma} - \sum_\beta t_{\gamma\beta} \cdot \xi_\beta,$$

wenn zur Abkürzung

$$\sum_\alpha a_{\gamma\alpha} \cdot \frac{1}{2} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}} = t_{\gamma\beta} \tag{100}$$

gesetzt wird; aus dieser Definitionsgleichung des Zeichens $t_{\gamma\beta}$ findet sich ohne Mühe die Beziehung

$$t_{\beta\gamma} + t_{\gamma\beta} = 0. \tag{101}$$

Wenn man dann die Gleichungen (98) mit Veränderung des Index folgendermassen schreibt:

$$x_\beta = \xi_\beta - \sum_\delta \xi_\delta \cdot \frac{1}{2} \frac{\partial f(s_{\beta i})}{\partial s_{\beta\delta}},$$

darauf mit

$$t_{\gamma\beta} = \sum_{\alpha} a_{\gamma\alpha} \cdot \frac{1}{2} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}}$$

multiplicirt und endlich über alle Werthe des Index β summirt, so ergiebt sich

$$\sum_{\beta} t_{\gamma\beta} x_{\beta} = \sum_{\beta} t_{\gamma\beta} \xi_{\beta} - \sum_{\alpha,\beta,\delta} a_{\gamma\alpha} \xi_{\delta} \cdot \frac{1}{4} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}} \frac{\partial f(s_{\beta i})}{\partial s_{\beta\delta}}$$

und durch Addition dieser Gleichung zur erstgefundenen folgt

$$\frac{1}{2} \frac{\partial f(x_i)}{\partial x_{\gamma}} + \sum_{\beta} t_{\gamma\beta} x_{\beta} = \frac{1}{2} \frac{\partial f(\xi_i)}{\partial \xi_{\gamma}} - \sum_{\alpha,\beta,\delta} a_{\gamma\alpha} \xi_{\delta} \cdot \frac{1}{4} \frac{\partial f(s_{\alpha i})}{\partial s_{\alpha\beta}} \frac{\partial f(s_{\beta i})}{\partial s_{\beta\delta}} .$$

Genau zu demselben Werthe gelangt man aber auf demselben Wege auch für den Ausdruck

$$\frac{1}{2} \frac{\partial f(x_i')}{\partial x_{\gamma}'} + \sum_{\beta} t_{\beta\gamma} x_{\beta}'$$

und somit geht folgendes System von Gleichungen

$$(102) \qquad \frac{1}{2} \frac{\partial f(x_i)}{\partial x_{\gamma}} + \sum_{\beta} t_{\gamma\beta} x_{\beta} = \frac{1}{2} \frac{\partial f(x_i')}{\partial x_{\gamma}'} + \sum_{\beta} t_{\beta\gamma} x_{\beta}'$$

als Resultat der Elimination der Variabeln ξ_{α} zwischen den Systemen (98) und (99) hervor.

Dass diese Formeln stets $f(x_i)$ in sich selbst transformiren, bestätigt man sogleich, indem man sie einmal mit x_{γ}, das andere Mal mit x_{γ}' multiplicirt und jedesmal über alle Werthe von γ summirt. So kommen die beiden Gleichungen

$$f(x_i) + \sum_{\beta,\gamma} t_{\gamma\beta} x_{\beta} x_{\gamma} = \sum_{\gamma} x_{\gamma} \cdot \frac{1}{2} \frac{\partial f(x_i')}{\partial x_{\gamma}'} + \sum_{\beta,\gamma} t_{\beta\gamma} x_{\gamma} x_{\beta}'$$

$$\sum_{\gamma} x_{\gamma}' \cdot \frac{1}{2} \frac{\partial f(x_i)}{\partial x_{\gamma}} + \sum_{\beta,\gamma} t_{\gamma\beta} x_{\beta} x_{\gamma}' = f(x_i') + \sum_{\beta,\gamma} t_{\beta\gamma} x_{\beta}' x_{\gamma}',$$

deren Addition mit Rücksicht einerseits auf die Formel (43), andererseits auf die Beziehung (101) sofort die Behauptung als richtig erkennen lässt. D i e G l e i c h u n g e n (102) s t e l l e n d e m n a c h e i n e T r a n s f o r m a t i o n d e r F o r m $f(x_i)$ i n s i c h s e l b s t v o r, enthalten in der That $\frac{n(n-1)}{2}$ Unbestimmte $t_{\beta\gamma}$

und haben, da $a_{\alpha\beta} = a_{\beta\alpha}$ ist, die Gestalt einer antisymmetrischen Substitution.

Nennt man t das alternirende System der n^2 Grössen $t_{\gamma\delta}$, so ist das System der Coefficienten auf der linken Seite von (102) das System $a + t$, auf der rechten Seite das System $a - t$. Um die Substitution in entwickelter Gestalt zu erhalten, müssten die Gleichungen (102) nach den x_α aufgelöst werden, was nur geschehen kann, wenn die Determinante des Systems $a + t$ von Null verschieden ist. Unter dieser Voraussetzung wird in der entwickelten Gestalt der Substitution das Coefficientensystem das folgende sein:

$$q = (a + t)^{-1} \cdot (a - t),$$

eine Beziehung, aus welcher weiter

$$(a + t) \cdot q = (a - t) \cdot e$$

also

$$(a + t) \cdot (e + q) = 2a \tag{103}$$

folgt. Somit gelangen wir zu nachfolgendem Satze: Ist a ein symmetrisches System von nicht verschwindender Determinante, t aber ein beliebiges alternirendes System, für welches die Determinante von $a + t$ nicht Null ist, so ist die Substitution (26) eine eigentliche*) Transformation der quadratischen Form $f(x_i)$ in sich selbst, wenn ihr Coefficientensystem q durch die Formel

$$q = (a + t)^{-1} \cdot (a - t) \tag{104}$$

bestimmt ist, und wegen (103) ist die Determinante von $e + q$ nicht Null oder die zur Substitution gehörige Fundamentalgleichung

$$e\lambda - q = 0$$

hat nicht die Wurzel $\lambda = -1$**).

Wenn nun aber auch die Hermite'schen Transformationen (102) die Bedingung erfüllen, $\frac{n(n-1)}{2}$ willkürliche Parameter

*) Offenbar ist $a + t = a - t$ also $Q = +1$.

**) S. hierzu und zum Folgenden Frobenius' genannte Abhandlung im Journ. f. Math. 84 S. 37 u. ff.

zu enthalten, so folgt daraus allein doch noch nicht, dass sie die allgemeine Lösung der Aufgabe, nämlich sämmtliche eigentliche Transformationen der Form $f(x_i)$ in sich selbst liefern. Es ist mithin auch noch fraglich, ob jede solche Transformation die Gestalt einer antisymmetrischen Substitution haben muss. Man kann aber weiter folgenden Satz beweisen: Jede (eigentliche) Substitution q, welche eine quadratische Form $f(x_i)$ von nicht verschwindender Determinante in sich selbst transformirt und deren Fundamentalgleichung die Wurzel -1 nicht hat, lässt sich auf eine einzige Weise in der Gestalt (104), in welcher t ein (aus endlichen Elementen bestehendes) alternirendes System ist, und folglich auch in Gestalt einer antisymmetrischen Substitution darstellen. Denn, erfüllt das System q mit der Determinante $Q = 1$ die Bedingung

$$q' \cdot a \cdot q = a, \tag{105}$$

während die Determinante von $e + q$ nicht Null ist, so kann man ein bestimmtes System x (mit endlichen Elementen) angeben, welches der Gleichung

$$x \cdot (q + e) = 2a$$

Genüge leistet; setzt man daher

$$t = x - a,$$

so wird

$$(a + t) \cdot (q + e) = 2a. \tag{106}$$

Aus dieser Gleichung erschliesst man zunächst, dass die Determinante von $a + t$ nicht Null sein kann. Schreibt man sodann die Gleichung in der Gestalt

$$(a + t)(q + e) = (a + t)e + (a - t)e,$$

so folgt weiter

$$q = (a + t)^{-1} \cdot (a - t)$$

und es bleibt nur zu zeigen, dass das System t ein alternirendes ist. Hierzu schreiben wir die Gleichung (106) folgendermassen:

$$t(q + e) = a - aq$$

und folgern daraus mit Rücksicht auf (105)

$$(q' + e)t(q + e) = q'a - aq.$$

Beim Uebergang zu den conjugirten Systemen geht

$$(q' + e)t'(q + e) = aq - q'a$$

d. h.

$$t' = -t$$

hervor, w. z. b. w.

Diesem Satze zufolge kann es sich nur noch darum handeln, ob es auch solche Transformationen der Form $f(x_i)$ in sich selbst giebt, bei welchen die Determinante von $q + e$ verschwindet und, falls dies zu bejahen ist, sie sämmtlich anzugeben. Was den ersteren Punkt betrifft, bemerken wir, dass, wenn wir

$$t_{\alpha\beta} = \frac{u_{\alpha\beta}}{\theta}$$

setzen, die Formel (104) die Gestalt

$$(104a) \qquad q = (a\theta + u)^{-1} \cdot (a\theta - u)$$

erhält, wodurch die Coefficienten der Substitution (26) d. i. die Elemente von q als homogene ganze Funktionen der $\frac{n(n-1)}{2} + 1$ Grössen $u_{\alpha\beta}$ und θ dargestellt werden. Da diese Coefficienten die Transformationsrelationen also algebraische Gleichungen befriedigen, sobald die $t_{\alpha\beta}$ endliche Werthe haben, werden sie ihnen auch Genüge leisten, wenn diese Grössen, indem θ gegen Null convergirt, unendlich wachsen. Alsdann gelangt man aber nothwendig zu Transformationen, bei denen $|q + e|$ Null werden muss, denn andernfalls würden sich aus (103) endliche Werthe für die $t_{\alpha\beta}$ ergeben. — Nachdem so der erste Punkt bejahend beantwortet worden, bleibt der zweite zu erledigen. Im zweiten Capitel des ersten Abschnittes ist gezeigt worden, dass bei ternären Formen auf dem eben angegebenen Wege sich sämmtliche Transformationen der in Rede stehenden besonderen Art ergeben. Indessen bilden diese Formen, wie Frobenius gezeigt hat, einen Ausnahmefall. Allgemein dagegen gilt der folgende von ihm (a. a. O. S. 43) hergeleitete Satz:

Jede Substitution (26), welche die Form $f(x_i)$ von

nicht verschwindender Determinante eigentlich in sich selbst transformirt, und für welche die Determinante von $q + e$ verschwindet, wird durch eine Formel

$$q = \lim_{\theta = 0} (a + t_\theta)^{-1} \cdot (a - t_\theta)$$

gegeben, in welcher t_θ ein alternirendes System bedeutet, dessen Elemente rationale Funktionen von θ sind.

Wir müssen uns jedoch versagen, die Schlüsse, durch welche Frobenius den Satz begründet hat, hier zu entwickeln. Schon haben wir weiter, als die arithmetische Theorie der quadratischen Formen es erfordert, ihren algebraischen Transformationen unsere Betrachtung gewidmet, um zu zeigen, wie die bezüglichen Untersuchungen des ersten Abschnitts, deren wir dort als Grundlage für das fünfte Capitel desselben bedurften, in der allgemeinen Theorie sich gestalten. Aber die Arithmetik der quadratischen Formen hat im Grunde nur an den ganzzahligen Transformationen ein Interesse. Noch liegen keine Untersuchungen darüber vor, welchen Bedingungen die unbestimmten Parameter $t_{\alpha\beta}$ in den algebraischen Formeln zu unterwerfen sein würden, um jene ganzzahligen Transformationen zu liefern, kaum kann man auch hoffen, auf solchem Wege zu den letzteren zu gelangen. Was man gegenwärtig bereits von den ganzzahligen Transformationen weiss, werden wir an einer späteren Stelle*) auseinandersetzen.

11. Wir haben noch eine Reihe algebraischer Hilfsbetrachtungen von einer etwas anderen Richtung anzufügen.

Zunächst erhalten wir durch eine blosse Verallgemeinerung der Determinantenbeziehung (15) im ersten Capitel des ersten Abschnitts die Verallgemeinerung der dort als eine der zwei Grundformeln bezeichneten Gleichung (17). Wir wollen diese auch hier als Grundformel bezeichnen, obwohl wir nicht den gleich umfassenden Gebrauch davon machen werden, wie in der einfacheren Theorie. Sie lautet folgendermassen:

$$(107)\quad f(x_i)\cdot f(y_i) - \Big(\sum_\alpha x_\alpha \cdot f^\alpha(y_i)\Big)^2 = f^{(2)}(x_\alpha y_\beta - x_\beta y_\alpha),$$

---

*) Im dritten Abschnitte.

wo $f^{(2)}$ die zweite Begleitform von f und ihre $\frac{n(n-1)}{2}$ Variabeln $x_\alpha y_\beta - x_\beta y_\alpha$ erhalten werden, indem man α die Werthe

$$1, 2, \cdots n-1$$

und β jedesmal alle grösseren Werthe der Reihe $2, 3, \cdots n$ durchlaufen lässt.

Den ersten Gebrauch machen wir von dieser Grundformel, um den wichtigen Satz herzuleiten, dass eine quadratische Form $f(x_i)$ mit n Veränderlichen, mit reellen Coefficienten und einer nicht verschwindenden Determinante durch eine reelle Substitution in ein Aggregat von n positiven oder negativen Quadraten von reellen Linearformen transformirt werden kann. In der That, da die Determinante nicht Null ist, kann die Form nicht identisch, d. h. nicht ihre sämmtlichen Coefficienten verschwinden; mithin kann man den Veränderlichen solche Werthe $\xi_1, \xi_2, \cdots \xi_n$ beilegen, dass die Form einen von Null verschiedenen Werth erhält; denn entweder ist einer der Hauptcoefficienten d. i. der Coefficient des Quadrats einer der Veränderlichen, z. B. a_{11}, von Null verschieden, oder, wenn diese sämmtlich Null wären, so würde der Coefficient eines der doppelten Produkte zweier Veränderlichen, z. B. a_{12}, nicht Null sein; im ersteren Falle genügt man der Forderung, wenn man $x_1 = 1$, im zweiten, wenn man $x_1 = 1$, $x_2 = 1$, alle übrigen x_α aber gleich Null setzt. Man kann, wie hieraus zu ersehen, die Werthe $\xi_1, \xi_2, \cdots \xi_n$ sogar als ganze Zahlen ohne gemeinsamen Theiler wählen, was besonders mit Rücksicht auf die späteren arithmetischen Anwendungen hervorgehoben werden soll. Zudem folgt hieraus, nach Cap. 3 nr. 5, dass man eine (reelle) unimodulare Substitution angeben kann, in welcher $\xi_1, \xi_2, \cdots \xi_n$ die erste Spalte des Coefficientensystems vorstellen, und durch diese Substitution geht $f(x_i)$ in eine andere (äquivalente) Form $g(x_i')$ über, deren erster Coefficient

$$b_{11} = f(\xi_i)$$

also von Null verschieden ist. Auf diese Form wenden wir die Grundformel an, indem wir in ihr $y_1 = 1$, die übrigen y_α

gleich Null wählen, und erhalten so die Gleichung

$$(108)\quad b_{11}\cdot f(x_i) = b_{11}\cdot g(x_i') = X_1^2 + g^{(2)}(x_2', x_3', \cdots x_n', 0\cdots),$$

in welcher $g^{(2)}$ nur noch von den $n-1$ Veränderlichen

$$x_2', x_3' \cdots x_n'$$

abhängt, die ihrerseits, ebenso wie

$$(109)\quad X_1 = b_{11}x_1' + b_{12}x_2' + \cdots + b_{1,n-1}x_{n-1}' + b_{1n}x_n',$$

reelle Linearformen der ursprünglichen Veränderlichen sind. Da die Form zur Rechten von (108) durch die Substitution (109) mit dem Modulus b_{11} sich in $b_{11}\,g(x_i')$ verwandelt, so ist ihre Determinante, d. i. die Determinante der Form

$$g^{(2)}(x_2', x_3', \cdots x_n', 0, \cdots),$$

gleich b_{11}^{n-2} mal derjenigen von $g(x_i')$ d. i. derjenigen von $f(x_i)$, also von Null verschieden. Man kann folglich auf vorstehende Form von Neuem dieselbe Betrachtung anwenden, die wir für $f(x_i)$ ausgeführt haben; und wenn man in dieser Weise weiter fortfährt und mit den dabei zur Anwendung kommenden, von Null verschiedenen Multiplikatoren $b_{11}, \cdots$ dividirt, erhält man offenbar zuletzt $f(x_i)$ mittels reeller Substitutionen von nicht verschwindendem Modulus dargestellt in der Gestalt

$$(110)\qquad f(x_i) = m_1X_1^2 + m_2X_2^2 + \cdots + m_nX_n^2.$$

Darin sind $X_1, X_2, \cdots X_n$ n unabhängige Linearformen mit den ursprünglichen Veränderlichen. Denn, da die Substitution, welche $f(x_i)$ in diese Gestalt bringt, von nicht verschwindendem Modulus ist, muss, wenn man

$$X_\alpha = p_{\alpha 1}x_1 + p_{\alpha 2}x_2 + \cdots + p_{\alpha n}x_n$$
$$(\alpha = 1, 2, \cdots n)$$

setzt, auch die Determinante dieser n Gleichungen von Null verschieden sein. —

Nach (69) ist ferner die Determinante der rechten Seite von (110), nämlich

$$m_1 m_2 \cdots m_n,$$

bis auf einen von Null verschiedenen quadratischen Faktor gleich der Determinante von $f(x_i)$ also von Null verschieden. Somit ist auch jede der Zahlen m_α von Null verschieden; setzt

man also

$$m_\alpha = \varepsilon_\alpha \cdot \mu_\alpha,$$

wo

$$\mu_\alpha > 0, \quad \varepsilon_\alpha = \pm 1$$

ist, so kann endlich

$$(111) \quad f(x_i) = \varepsilon_1 (X_1 \sqrt{\mu_1})^2 + \varepsilon_2 (X_2 \sqrt{\mu_2})^2 + \cdots + \varepsilon_n (X_n \sqrt{\mu_n})^2$$

d. h., wie behauptet, gleich einem Aggregat von n positiven oder negativen Quadraten reeller Linearformen mit den Veränderlichen $x_1, x_2, \cdots x_n$ gesetzt werden.

Man bemerke hier sogleich Folgendes: Sind die Coefficienten der Form $f(x_i)$ ganze Zahlen, so werden, der getroffenen Wahl der Zahlen $\xi_1, \xi_2, \cdots \xi_n$ gemäss nicht nur b_{11} und die Coefficienten der Form $g^{(2)}$, sondern auch diejenigen der Linearform X_1 ganzzahlig sein. Da bei dem Fortgange der Transformation ähnliches gelten muss, lässt sich für diesen Fall der bewiesene Satz folgendermassen aussprechen: Ist $f(x_i)$ eine quadratische Form mit n Veränderlichen, mit ganzzahligen Coefficienten und einer von Null verschiedenen Determinante, so kann man sie, mit einer von Null verschiedenen ganzen Zahl M multiplicirt, stets auf die Form bringen:

$$(112) \qquad M \cdot f(x_i) = m_1 X_1^2 + m_2 X_2^2 + \cdots + m_n X_n^2,$$

in welcher $m_1, m_2, \cdots m_n$ positive oder negative ganze Zahlen, die X_γ aber n unabhängige homogene lineare Funktionen der Veränderlichen $x_1, x_2, \cdots x_n$ mit ganzzahligen Coefficienten sind.

12. Wir wollen nun einen andern Weg einschlagen, zur Darstellung (110) zu gelangen, auf welchem die Zahlen

$$m_1, m_2, \cdots m_n$$

sogleich durch die Coefficienten der Form $f(x_i)$ ausgedrückt erhalten werden. Jacobi hat zuerst diese Aufgabe allgemein gelöst*). Hier soll der Gang eingehalten werden, welchen

*) Jacobi, über eine elementare Transformation eines in Bezug auf jedes von zwei Variabelnsystemen linearen und homogenen Ausdrucks, aus seinen hinterlassenen Papieren herausg. v. Borchardt, im Journ. f. Math. 53 S. 265.

Gundelfinger in Verfolgung eines Plücker'schen Grundgedankens angegeben hat*). Sei

$$f(x_i) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha x_\beta$$

die quadratische Form und ihre Determinante A von Null verschieden; mit $A_{\alpha\beta}$ werde das zu $a_{\alpha\beta}$ adjungirte Element dieser Determinante bezeichnet. Ist nun $A_{nn} = \frac{\partial A}{\partial a_{nn}}$ von Null verschieden, so geht $f(x_i)$ durch die Substitution

$$\text{(113a)} \quad \begin{cases} x_\gamma = x_\gamma' + \frac{A_{n\gamma}}{A_{nn}} \cdot X_n \\ \quad (\gamma = 1, 2, \cdots n-1) \\ x_n = X_n \end{cases}$$

über in die Gestalt

$$\text{(114a)} \qquad \sum_{(\gamma, \delta = 1, 2, \cdots n-1)} a_{\gamma\delta} x_\gamma' x_\delta' + \frac{A}{A_{nn}} \cdot X_n^2.$$

Denn aus (113a) folgen unmittelbar die Gleichungen

$$\text{(115)} \quad \begin{cases} a_{\gamma 1} x_1 + a_{\gamma 2} x_2 + \cdots + a_{\gamma n} x_n \\ = a_{\gamma 1} x_1' + \cdots + a_{\gamma, n-1} x_{n-1}' \\ \quad (\gamma = 1, 2, \cdots n-1) \\ a_{n1} x_1 + a_{n2} x_2 + \cdots + a_{nn} x_n \\ = a_{n1} x_1' + \cdots + a_{n, n-1} x_{n-1}' + \frac{A}{A_{nn}} X_n, \end{cases}$$

und durch Multiplikation der $n-1$ ersten dieser Gleichungen mit $x_1, x_2, \cdots x_{n-1}$, der letzten mit x_n und durch darauffolgende Addition ergiebt sich mit Rücksicht auf die Gleichheit $a_{\alpha\beta} = a_{\beta\alpha}$

$$f(x_i) = \sum_{(\delta = 1, 2, \cdots n-1)} (a_{\delta 1} x_1 + \cdots + a_{\delta n} x_n) x_\delta' + \frac{A}{A_{nn}} X_n x_n$$

d. i. bei Benutzung der Gleichungen (115) und wegen $x_n = X_n$ die Gleichung

$$f(x_i) = \sum_{(\gamma, \delta = 1, 2, \cdots n-1)} a_{\gamma\delta} x_\gamma' x_\delta' + \frac{A}{A_{nn}} X_n^2.$$

---

*) Gundelfinger, zur Theorie der quadratischen Formen, Journ. f. Math. 91 S. 221.

Die quadratische Form

$$(116a)\qquad \sum_{(\gamma,\delta=1,2,\cdots n-1)} a_{\gamma\delta}\, x_\gamma'\, x_\delta'$$

hat zudem die von Null verschiedene Determinante A_{nn}. Das in der Darstellung (114a) auftretende Quadrat X_n^2 hat einen positiven oder negativen Coefficienten, jenachdem A, A_{nn} gleichen oder verschiedenen Vorzeichens sind.

Ist aber $A_{nn}=0$, so muss, da

$$A = a_{n1}A_{n1} + a_{n2}A_{n2} + \cdots + a_{nn}A_{nn}$$

ist, eine der Unterdeterminanten $A_{n1}, A_{n2}, \cdots A_{n,n-1}$ von Null verschieden sein. Nehmen wir $A_{n,n-1} \gtrless 0$ an. Dann geht die quadratische Form $f(x_i)$ durch die Substitution

$$(113b)\qquad \begin{cases} x_\gamma = x_\gamma' + \dfrac{A_{n\gamma}}{A_{n,n-1}}\cdot x_{n-1} \\ \qquad (\gamma = 1, 2, \cdots n-2) \\ \dfrac{A}{A_{n,n-1}} x_{n-1} = \dfrac{1}{2}\left(\dfrac{A}{A_{n,n-1}} + a_{nn}\right) X_n \\ \qquad + \dfrac{1}{2}\left(\dfrac{A}{A_{n,n-1}} - a_{nn}\right) X_{n-1} \\ \qquad - a_{n1}x_1' - a_{n2}x_2' - \cdots - a_{n,n-2}x_{n-2}' \\ x_n = X_{n-1} - X_n, \end{cases}$$

wie durch analoge Betrachtungen bestätigt wird, in die Gestalt

$$(114b)\qquad \sum_{(\gamma,\delta=1,2,\cdots n-2)} a_{\gamma\delta}\, x_\gamma'\, x_\delta' + \frac{A}{A_{n,n-1}}(X_{n-1}^2 - X_n^2)$$

über. Der Gleichung

$$(117)\qquad A\cdot\frac{\partial^2 A}{\partial a_{nn}\,\partial a_{n-1,n-1}} = A_{nn}\,A_{n-1,n-1} - A_{n,n-1}^2$$

zufolge ist zudem die Determinante der quadratischen Form

$$(116b)\qquad \sum_{(\gamma,\delta=1,2,\cdots n-2)} a_{\gamma\delta}\, x_\gamma' x_\delta',$$

nämlich die Unterdeterminante $\dfrac{\partial^2 A}{\partial a_{nn}\,\partial a_{n-1,n-1}}$, von Null verschieden. Von den beiden in (114b) auftretenden Quadraten X_n^2, X_{n-1}^2 hat nothwendig eins und nur eins einen negativen

Coefficienten, aus (117) aber folgt, dass

$$A \text{ und } \frac{\partial^2 A}{\partial a_{nn}\,\partial a_{n-1,n-1}}$$

entgegengesetzten Vorzeichens sind, dass also die drei Unterdeterminanten

$$A, \frac{\partial A}{\partial a_{nn}}, \frac{\partial^2 A}{\partial a_{nn}\,\partial a_{n-1,n-1}},$$

deren mittlere verschwindet also bei der Zählung der Zeichenwechsel nicht zu beachten ist, einen Zeichenwechsel darbieten.

Auf die Form (116a) oder (116b) lässt sich nun wieder die eine oder die andere der beiden angegebenen Umformungen zur Anwendung bringen. Der weitere Fortgang dieser Betrachtung aber führt, wenn wir von den speciellen, von uns gemachten Voraussetzungen, dass von den Unterdeterminanten gerade die Determinanten A_{nn}, resp. $A_{n,n-1}$ von Null verschieden seien, absehen, wie unmittelbar zu erkennen ist, zu folgendem Satze: Wählt man — was das Gesagte als thunlich übersehen lässt — die Reihe der Determinanten

$$(118)\qquad A, \frac{\partial A}{\partial a_{\alpha\alpha}}, \frac{\partial^2 A}{\partial a_{\alpha\alpha}\,\partial a_{\beta\beta}}, \frac{\partial^3 A}{\partial a_{\alpha\alpha}\,\partial a_{\beta\beta}\,\partial a_{\gamma\gamma}}, \cdots a_{\nu\nu}, 1$$

der Art, dass in ihr keine zwei aufeinanderfolgenden zugleich verschwinden, so lässt sich die quadratische Form $f(x_i)$ als ein Aggregat von n Quadraten von reellen homogenen linearen Funktionen der Veränderlichen $x_1, x_2, \cdots x_n$ in der Gestalt (110) darstellen, in welcher genau so viel Quadrate negative Coefficienten haben, als die Reihe (118) nach Ausfall der verschwindenden Glieder Zeichenwechsel darbietet.

Sind insbesondere die Determinanten

$$(118\text{a})\qquad A, \frac{\partial A}{\partial a_{nn}}, \frac{\partial^2 A}{\partial a_{nn}\,\partial a_{n-1,n-1}}, \cdots a_{11}, 1$$

die wir kurz die Determinanten

$$A_n, A_{n-1}, A_{n-2}, \cdots A_1, 1$$

nennen wollen, von Null verschieden, so findet folgende Darstellung der Form $f(x_i)$ statt:

$$(119)\quad f(x_i) = A_1 X_1^2 + \frac{A_2}{A_1} X_2^2 + \cdots + \frac{A_{n-1}}{A_{n-2}} X_{n-1}^2 + \frac{A_n}{A_{n-1}} X_n^2;$$

und da in diesem Falle nur Substitutionen von der Art (113a) zur Anwendung kommen, erkennt man sogleich, dass X_n nur von x_n, X_{n-1} nur von x_{n-1}, x_n, u. s. w., allgemein X_α nur von $x_\alpha, x_{\alpha+1}, \cdots x_n$ abhängig sein wird. Diese Darstellung lehrte Jacobi a. a. O.*).

Man kann übrigens auch Formen mit verschwindender Determinante als Aggregat von Quadraten darstellen, deren Anzahl dann kleiner als n ist. Für unsere Zwecke dürfen wir jedoch diesen Fall übergehen. Man findet ihn, sowie auch denjenigen, in welchem die Veränderlichen nicht unabhängig von einander, sondern durch lineare Beziehungen mit einander verbunden sind, in der Arbeit von Gundelfinger, desgleichen in Darboux' in nr. 6 angezogener Abhandlung ausführlich behandelt. Auf die letztere Arbeit, in welcher die Transformation der quadratischen Formen in eine Quadratsumme unter sehr allgemeinem Gesichtspunkte behandelt wird, wollen wir noch besonders hinweisen, weil in ihr die in nr. 6 eingeführten Begleitformen ebenfalls und zwar in der Gestalt von Determinanten benutzt worden sind. In der That, die dort verwandten Determinanten von der Gestalt

$$\Phi_m = \begin{vmatrix} a_{11} & a_{12} & \cdots a_{1n} & x_1' & x_1'' & \cdots x_1^{(m)} \\ a_{21} & a_{22} & \cdots a_{2n} & x_2' & x_2'' & \cdots x_2^{(m)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots a_{nn} & x_n' & x_n'' & \cdots x_n^{(m)} \\ x_1' & x_2' & \cdots x_n' & 0 & 0 & \cdots 0 \\ x_1'' & x_2'' & \cdots x_n'' & 0 & 0 & \cdots 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1^{(m)} & x_2^{(m)} & \cdots x_n^{(m)} & 0 & 0 & \cdots 0 \end{vmatrix},$$

deren sich übrigens auch Gundelfinger zu seiner Untersuchung bedient, sind, wenn für irgend welche Combination von m Zahlen $h, i, k, \cdots$ der Reihe $1, 2, 3, \cdots n$

$$\begin{vmatrix} x_h' & x_h'' & \cdots x_h^{(m)} \\ x_i' & x_i'' & \cdots x_i^{(m)} \\ x_k' & x_k'' & \cdots x_k^{(m)} \\ \cdot & \cdot & \cdot \end{vmatrix} = \begin{vmatrix} x_h' & x_i' & x_k' & \cdots \\ x_h'' & x_i'' & x_k'' & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ x_h^{(m)} & x_i^{(m)} & x_k^{(m)} & \cdots \end{vmatrix} = (-1)^{h+i+k\cdots} \cdot \xi_{hik\cdots}$$

*) Hermite (Journ. f. Math. 47 S. 332) schreibt sie Cauchy zu.

gesetzt wird, mit dem folgenden Ausdrucke

$$\Phi_m = (-1)^m \cdot f^{(n-m)}(\xi_{hix}\ldots),$$

wie sehr einfach zu übersehen ist, identisch.

13. Nachdem wir im Vorigen auf verschiedene Weise die Möglichkeit hergeleitet, die Form $f(x_i)$ in der Gestalt (110) darzustellen, erübrigt noch für unsere Zwecke, einen überaus bedeutsamen Zusatz zu beweisen. Dieser Zusatz sagt aus, dass, auf welche Weise immer jene Darstellung bewerkstelligt werden mag, die Anzahl der Quadrate, deren Coefficienten positiv bezw. negativ sind, jedesmal dieselbe sein muss. Das hierin ausgesprochene Gesetz ist von Sylvester das Trägheitsgesetz der quadratischen Formen genannt worden. Wie eine aus den hinterlassenen Papieren Jacobi's von Borchardt herausgegebene Arbeit ausweist*), ist dies Gesetz Jacobi nicht nur bereits bekannt gewesen, sondern auch auf die einfachste Art von ihm bewiesen worden. Jedoch hat Sylvester zuerst es öffentlich bekannt gemacht**). Nach diesem ist es von Hermite***) bewiesen worden; einen anderen, sehr instructiven Beweis gab Brioschi†). Wir müssen uns damit begnügen, hier den Jacobi'schen Beweis auseinanderzusetzen.

Gesetzt, $f(x_i)$ werde einmal als Aggregat von Quadraten mit μ positiven und ν negativen Coefficienten dargestellt, sodass

$$\mu + \nu = n$$

*) Jacobi, über einen algebraischen Fundamentalsatz und seine Anwendungen, Fragment; Journ. f. Math. 53 S. 275. Nach Borchardt dürfte dieses Fragment aus dem Jahre 1847 stammen.

**) Sylvester, Phil. Magaz. 1852 II S. 138, A Demonstration of the Theorem, that every homogeneous quadratic polynomial is reductible by real orthogonal substitutions to the form of a sum of positive and negative squares; sowie Phil. Trans. 1853 S. 481, 484.

***) Hermite, extrait d'une lettre de Mr. Ch. Hermite à Mr. Borchardt sur l'invariabilité des nombres des carrés positifs et des carrés negatifs dans la transformation des polynomes homogènes du second degré, Journ. f. Math. 53 S. 271. Vgl. Serret, Handbuch der Algebra, deutsch von Wertheim 1. Theil S. 444.

†) Brioschi, sur les séries qui donnent le nombre de racines réelles etc., in Nouv. Ann. de Mathém. de Terquem, t. 15 (1856) p. 264.

ist. Nach (111) lässt sich dann schreiben

$$f(x_i) = u_1^2 + u_2^2 + \cdots + u_\mu^2 - v_1^2 - v_2^2 - \cdots - v_\nu^2,$$

wo die u, v Linearformen mit den Veränderlichen $x_1, x_2, \cdots x_n$ sind. Wird $f(x_i)$ ein andermal als ein Aggregat von Quadraten gefunden, unter deren Coefficienten λ positiv, ϱ negativ sind, sodass

$$\lambda + \varrho = n$$

ist, so fände man nach (111)

$$f(x_i) = u_1'^2 + u_2'^2 + \cdots + u_\lambda'^2 - v_1'^2 - v_2'^2 - \cdots - v_\varrho'^2,$$

wo auch die u', v' Linearformen mit den Veränderlichen $x_1, x_2, \cdots x_n$ sind. Dann müsste also eine Gleichung bestehen

$$(120)\quad \begin{cases} \quad u_1^2 + u_2^2 + \cdots + u_\mu^2 - v_1^2 - v_2^2 - \cdots - v_\nu^2 \\ = u_1'^2 + u_2'^2 + \cdots + u_\lambda'^2 - v_1'^2 - v_2'^2 - \cdots - v_\varrho'^2, \end{cases}$$

und es ist nun zu zeigen, dass eine solche Gleichung nicht anders möglich ist, als wenn

$$\lambda = \mu, \quad \nu = \varrho$$

ist.

Hierzu dient die folgende einfache Bemerkung. Sind

$$A_1, A_2, \cdots A_i$$

i unabhängige Linearformen mit den Veränderlichen $x_1, x_2, \cdots x_n$, was $i \overline{\overline{<}} n$ voraussetzt, sind ebenso

$$B_1, B_2, \cdots B_m$$

m Linearformen mit diesen Veränderlichen und unter ihnen $\varkappa \overline{\overline{<}} m$ — nehmen wir an, die ersten $\varkappa$ — von einander unabhängig, was auch $\varkappa \overline{\overline{<}} n$ voraussetzt, so kann man $\varkappa$ der Veränderlichen — nehmen wir an, die $\varkappa$ ersten derselben — durch die $\varkappa$ unabhängigen unter den Linearformen B_α und die $n - \varkappa$ übrigen x_α linear ausdrücken und demnach jede der Linearformen A_α auf die Form bringen

$$A_\alpha = b_1^\alpha B_1 + b_2^\alpha B_2 + \cdots + b_\varkappa^\alpha B_\varkappa + c_{\varkappa+1}^\alpha x_{\varkappa+1} + \cdots + c_n^\alpha x_n.$$
$$(\alpha = 1, 2, \cdots i)$$

Darin werden, so oft $\varkappa < i$ ist, nicht sämmtliche $c_{\varkappa+1}^\alpha, \cdots c_n^\alpha$ Null sein können, da sonst die i unabhängigen Linearformen

A_α aus nur $\varkappa < i$ Veränderlichen $B_1, B_2, \cdots B_\varkappa$ zusammengesetzt wären; aus diesem Grunde wird man die Veränderlichen $x_1, x_2, \cdots x_n$ so wählen können, dass, während $B_1, B_2, \cdots B_\varkappa$ also auch die sämmtlichen übrigen Linearformen B_α verschwinden, nicht zugleich auch die sämmtlichen i Linearformen A_α zu Null werden.

Wäre nun in der Gleichung (120) λ von μ verschieden, etwa $\lambda > \mu$, so wäre auch $\lambda + \varrho > \mu + \varrho$ und somit würde man die Veränderlichen $x_1, x_2, \cdots x_n$ so wählen können, dass, während die Linearformen $u_1, u_2, \cdots u_\mu, v_1', v_2', \cdots v_\varrho'$ verschwinden, nicht zugleich auch die sämmtlichen, nach einer oben gemachten Bemerkung von einander unabhängigen Linearformen $u_1', u_2', \cdots u_\lambda'$ zu Null werden. Die Gleichung (120) wäre dann aber unmöglich. Ebensowenig kann $\lambda < \mu$ sein, mithin muss $\lambda = \mu$ und somit auch $\varrho = \nu$ sein, w. z. b. w.

Von diesem fundamentalen Gesetze hat schon Jacobi — wie die Bemerkungen Borchardt's im Journ. f. Math. 53 S. 281 u. ff. zeigen — eine sehr wichtige Anwendung auf die Lehre von den reellen algebraischen Gleichungen gemacht, um die Anzahl ihrer reellen und ihrer imaginären Wurzeln festzustellen. In der That, wenn $\alpha_1, \alpha_2, \cdots \alpha_n$ die Wurzeln einer Gleichung n^{ten} Grades mit reellen Coefficienten und $f(x_i)$ die auf alle diese Wurzeln α bezogene Summe

$$(121) \quad f(x_i) = \sum_\alpha (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^2$$

bezeichnen, so lässt sich dieser Ausdruck in entwickelter Gestalt als eine quadratische Form mit den n Veränderlichen $x_0, x_1, \cdots x_{n-1}$ auch folgendermassen darstellen:

$$(121\text{a}) \qquad f(x_i) = \sum_{(\alpha, \beta = 0, 1, 2, \cdots n-1)} s_{\alpha+\beta} \cdot x_\alpha x_\beta,$$

wenn unter $s_\varkappa$ die Summe der $\varkappa^{\text{ten}}$ Potenzen aller Wurzeln:

$$s_\varkappa = \alpha_1^\varkappa + \alpha_2^\varkappa + \cdots + \alpha_n^\varkappa$$

verstanden wird. Nun ist erstens jedes Glied der Summe (121), welches auf eine reelle Wurzel α sich bezieht, das positive Quadrat einer Linearform. Dagegen geben je zwei Glieder, welche conjugirt-imaginären Wurzeln entsprechen,

zusammengenommen eine Differenz $P^2 - Q^2$ zweier solcher Quadrate, geben also Anlass zu je einem negativen Quadrate, und folglich ist die Anzahl der negativen Quadrate in der ersten Darstellung (121) der quadratischen Form als Aggregat von Quadraten von n Linearformen genau so gross, wie die Anzahl der Paare conjugirt imaginärer Wurzeln, welche die Gleichung n^{ten} Grades hat.

Zweitens aber lässt sich die Form (121a) nach der Formel

$$f(x_i) = A_0 X_0^2 + \frac{A_1}{A_0} X_1^2 + \cdots + \frac{A_{n-1}}{A_{n-2}} X_{n-1}^2$$

als Aggregat von Quadraten von n Linearformen darstellen, wenn gesetzt wird

$$(122)\qquad A_0 = s_0, \quad A_1 = \begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}, \quad A_2 = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} \quad \text{u. s. w.}$$

und hat in dieser Gestalt genau so viel negative Quadrate, als die Anzahl der Zeichenwechsel in der Reihe (122) beträgt. Dem Jacobi-Sylvester'schen Trägheitsgesetze gemäss ist folglich zu schliessen:

Die Anzahl der Paare conjugirt imaginärer Wurzeln der Gleichung n^{ten} Grades mit reellen Coefficienten ist ebenso gross, wie die Anzahl der Zeichenwechsel in der Reihe (122).

Auch Sylvester und Hermite*) haben das Trägheitsgesetz der quadratischen Formen zu eingehenden Untersuchungen über die Anzahl reeller und imaginärer Wurzeln der algebraischen Gleichungen und die zu deren Bestimmung dienenden Sturm'schen Funktionen verwendet. Insbesondere hat der Zweitgenannte das Jacobi'sche Resultat nicht nur insofern erweitert, als er die Anzahl der reellen Wurzeln einer Gleichung nicht sowohl überhaupt, als vielmehr zwischen gegebenen Grenzen bestimmte, sondern er hat auch in einer sehr lesenswerthen Arbeit**) die Untersuchung auf Gleichungen mit

---

*) Vgl. in dieser Beziehung auch Darboux' obengenannte Abhandlung.

**) Hermite, extrait d'une lettre de Mr. Ch. Hermite de Paris

imaginären Coefficienten ausgedehnt und die Anzahl derjenigen ihrer Wurzeln, die innerhalb gegebener Gebiete enthalten sind und positive resp. negative imaginäre Bestandtheile haben, bestimmt. Es ist von höchstem Interesse, zu sehen, wie auf solche Weise mittels eines rein algebraischen Princips, ohne irgend welche Einmischung des Stetigen, die auf jene Anzahl bezüglichen Sätze gefunden werden können, welche vordem Cauchy aus seiner Theorie der complexen Integration erschlossen hatte.

14. Doch dürfen wir hier diese Folgerungen aus dem Trägheitsgesetze nicht weiter verfolgen, müssen dagegen eine andere herleiten, welche für unsere Zwecke erforderlich ist. Dies Gesetz lehrt nämlich offenbar sämmtliche quadratische Formen mit n Veränderlichen in verschiedene Typen zu unterscheiden, indem man alle diejenigen zu demselben Typus zählt, deren Darstellung als Aggregat von n Quadraten die gleiche Anzahl positiver sowie die gleiche Anzahl negativer Quadrate aufweist. Solcher verschiedenen Typen giebt es $n+1$, unter ihnen denjenigen Typus, der lauter positive, sowie denjenigen, der lauter negative Quadrate aufweist. Es leuchtet ein, dass Formen des ersten dieser zwei Typen nur positive, Formen des zweiten nur negative Werthe haben können, wenn — was stets geschehen soll — die Veränderlichen reell gedacht werden. Deshalb heissen Formen des erstgenannten Typus positive, Formen des zweitgenannten Typus negative, zusammengenommen die Formen dieser beiden Typen bestimmte Formen (formae definitae). Die Formen der übrigen Typen sind unbestimmte (formae indefinitae), denn sie können offenbar sowohl positive als negative Werthe annehmen. Unter dem Index oder Trägheitsindex τ eines jeden Typus wollen wir die Anzahl der *negativen* Quadrate verstehen, welche die Darstellung der Formen desselben als Aggregat von Quadraten aufweist, sodass dieser Trägheitsindex τ für positive Formen Null, für negative Formen gleich n ist.

à Mr. Borchardt de Berlin sur le nombre des racines d'une équation algébrique comprises entre des limites données, im J. f. Math. 52 S. 39.

Bestimmte Formen können stets nach der Jacobischen Formel (119) als Aggregat von Quadraten dargestellt werden. In der Reihe (118a) von Determinanten kann nämlich keine verschwinden; denn, wäre entgegengesetzten Falles A_{m-1} die erste dieser Determinanten, welche den Werth Null hat, so ginge $f(x_i)$, wenn

$$x_{m+1},\ x_{m+2},\ \cdots x_n$$

gleich Null gewählt werden, in die quadratische Form

$$\sum_{(\gamma,\delta=1,2,\cdots m)} a_{\gamma\delta}\, x_\gamma\, x_\delta$$

von m Veränderlichen mit der Determinante $A_m \gtrless 0$ über, während $\frac{\partial A_m}{\partial a_{m,m}} = 0$ wäre; auf diese Form liesse sich daher eine der zweiten Substitution in nr. 12 analoge Substitution anwenden, um sie in eine mit (114b) analoge Gestalt überzuführen, aus welcher ohne Weiteres zu ersehen ist, dass jene Form und somit auch — gegen die Annahme — $f(x_i)$ sowohl positive wie negative Werthe erhalten könnte.

Für positive Formen haben hiernach die Determinanten (118a) sämmtlich das positive Vorzeichen, ihre Reihe bietet also nur Zeichenfolgen, für negative Formen dagegen bietet diese Reihe lauter Zeichenwechsel dar.

Da die negativen Formen als mit entgegengesetztem Vorzeichen genommene positive aufgefasst werden dürfen, kann man die Betrachtung der bestimmten Formen offenbar auf die positiven Formen beschränken.

Die positiven (bestimmten) Formen haben die charakteristische Eigenschaft, dass, wenn der Werth der Form eine bestimmte Grenze nicht überschreitet, auch die Werthe der Veränderlichen unterhalb endlicher Grenzen verbleiben. In der That, ist $f(x_i)$ eine positive Form mit den n Veränderlichen $x_1, x_2, \cdots x_n$ und setzt man sie in die Gestalt (110):

$$f(x_i) = m_1 X_1^2 + m_2 X_2^2 + \cdots + m_n X_n^2,$$

worin

$$X_\alpha = p_{\alpha 1} x_1 + p_{\alpha 2} x_2 + \cdots + p_{\alpha n} x_n \qquad (123)$$
$$(\alpha = 1, 2, \cdots n)$$

ist, so folgt aus den letzteren Beziehungen, da die Determinante $| p_{\alpha\beta} |$ von Null verschieden ist, umgekehrt

$$x_\alpha = \varpi_{1\alpha} X_1 + \varpi_{2\alpha} X_2 + \cdots + \varpi_{n\alpha} X_n, \qquad (124)$$
$$(\alpha = 1, 2, \cdots n)$$

wo die $\varpi_{\alpha\beta}$ bestimmte endliche Werthe haben. Soll demnach

$$f(x_i) \overline{\gtrless} G \qquad (125)$$

sein, so muss

$$\text{abs. } X_\alpha \overline{\gtrless} \sqrt{\frac{G}{m_\alpha}}$$

folglich

$$\text{abs. } x_\alpha \overline{\gtrless} \sqrt{G}\left(\text{abs. } \frac{\varpi_{1\alpha}}{\sqrt{m_1}} + \text{abs. } \frac{\varpi_{2\alpha}}{\sqrt{m_2}} + \cdots + \text{abs. } \frac{\varpi_{n\alpha}}{\sqrt{m_n}}\right)$$
$$(\alpha = 1, 2, \cdots n)$$

sein, wie behauptet.

Hieraus folgt, dass die Ungleichheit (125) nur eine endliche Anzahl *ganzzahliger* Lösungen haben kann. Ist also insbesondere $f(x_i)$ eine ganzzahlige positive Form und G eine positive ganze Zahl, so hat diese letztere, wenn sie überhaupt durch die Form $f(x_i)$ mittels ganzzahliger Werthe der Veränderlichen darstellbar ist, stets nur eine *endliche Anzahl* solcher Darstellungen durch dieselbe.

Sechstes Capitel.

Classen, Ordnungen und Geschlechter quadratischer Formen.

1. Sobald man von der algebraischen Theorie der quadratischen Formen zu ihrer arithmetischen Theorie übergeht, darf man sich im allgemeinen auf den Fall beschränken, wo die Coefficienten der quadratischen Form, also auch ihre Determinante und deren sämmtliche Unterdeterminanten ganze Zahlen sind; auch werden nur Substitutionen mit ganzzahligen Coefficienten in Betracht

kommen. Die arithmetische Aequivalenz zweier solcher Formen besteht darin, dass eine von ihnen durch eine ganzzahlige Substitution mit dem Modulus 1 in die andere verwandelt werden kann, wo dann auch umgekehrt diese in jene in gleicher Weise sich verwandeln lässt. Aequivalente Formen stellen deshalb offenbar genau dieselben Zahlen dar, wenn man ihren Unbestimmten alle möglichen ganzzahligen Werthe ertheilt.

Alle unter einander äquivalenten Formen fassen wir in *eine Classe* zusammen. Nach nr. 7 vorigen Capitels haben sie alle dieselbe Determinante. Da von zwei äquivalenten Formen die eine durch eine reelle Substitution in die andere übergeht, müssen beide in dasselbe Aggregat von Quadraten überführbar also demselben Typus quadratischer Formen angehörig, und folglich auch für beide der Trägheitsindex τ derselbe sein. Die Anzahl der Classen äquivalenter Formen mit ein- und derselben Determinante ist endlich. Der Beweis dieses Satzes stützt sich auf die Eigenschaften der reducirten Formen und gehört somit zu dem Kreise von Betrachtungen, denen der dritte Abschnitt dieses Werkes gewidmet ist; er wird dort nachträglich geliefert werden.

Die Determinante der quadratischen Formen setzen wir stets von Null verschieden voraus.

Die sämmtlichen Coefficienten $a_{\alpha\beta}$ einer quadratischen Form

$$(1) \qquad f(x_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha x_\beta$$

von nicht verschwindender Determinante werden einen grössten (positiven) gemeinsamen Theiler haben, welcher d_0 heisse; die Zahlen $\frac{a_{\alpha\beta}}{d_0}$ haben dann keinen gemeinsamen von 1 verschiedenen Theiler mehr, wohl aber können die Zahlen

$$\frac{a_{\alpha\alpha}}{d_0} \text{ und } 2\frac{a_{\alpha\beta}}{d_0} \ (\alpha \gtrless \beta)$$

dann noch den gemeinsamen Theiler 2 haben, wenn nämlich die erstgenannten sämmtlich gerade sind; jenachdem dies der

Fall ist oder nicht, setzen wir $\sigma_1 = 2$ oder $\sigma_1 = 1$. Ist d_0 prim gegen eine gegebene Zahl N, so nennen wir die Form $f(x_\varrho)$ prim gegen N und, wenn $d_0 = 1$, eine primitive Form. Die Form $\frac{1}{d_0} \cdot f(x_\varrho)$ ist mithin stets primitiv. Wir unterscheiden die primitiven Formen in eigentlich und uneigentlich primitive, jenachdem bei ihnen $\sigma_1 = 1$ oder $\sigma_1 = 2$ ist, oder nennen sie kürzer entsprechend ungerade oder gerade Formen. Wo nicht ausdrücklich das Gegentheil gesagt wird, werden wir unsere Betrachtung auf primitive Formen einschränken.

Auf ganz analoge Weise wie im dritten Capitel des ersten Abschnitts erkennt man, dass durch eine ungerade primitive Form stets eine Zahl darstellbar ist, welche prim ist zu einer beliebig gegebenen Zahl N, durch eine gerade primitive Form aber das Doppelte einer solchen. Allgemeiner zeigt man aus den gleichen Gründen, dass dieser Satz auch für nicht-primitive Formen giltig bleibt, sobald sie nur prim sind gegen jene Zahl N. —

Betrachten wir nun die Begleitformen von $f(x_\varrho)$:

$$f^{(m)}(x_{\varrho\sigma\tau\ldots}) = \sum A^{(m)}_{hi\varkappa\ldots,rst\ldots} \cdot x_{hi\varkappa\ldots} \cdot x_{rst\ldots},$$

so können wir Aehnliches bemerken: jeder von ihnen kommt eine positive ganze Zahl d_{m-1} zu, welche grösster gemeinsamer Theiler aller ihrer Coefficienten $A^{(m)}_{hi\varkappa\ldots,rst\ldots}$ ist und eine Zahl σ_m gleich 1 oder gleich 2, welche der grösste gemeinsame Theiler der Zahlen

$$\frac{1}{d_{m-1}} \cdot A^{(m)}_{hi\varkappa\ldots,hi\varkappa\ldots} \text{ und } \frac{2}{d_{m-1}} \cdot A^{(m)}_{hi\varkappa\ldots,rst\ldots}$$

(für verschiedene Combinationen $hi\varkappa\cdots, rst\cdots$) ist. Offenbar ist d_{n-1} gleich dem absoluten Werthe der Determinante A der quadratischen Form, nämlich, wenn τ den Trägheitsindex der quadratischen Form $f(x_\varrho)$ bedeutet,

$$(2) \qquad d_{n-1} = (-1)^\tau \cdot A.$$

So erhält man bezüglich der quadratischen Form $f(x_\varrho)$ von n Veränderlichen die Zahlen

$$d_0,\ d_1,\ d_2 \cdots d_{n-1}$$
$$\sigma_1,\ \sigma_2 \cdots \sigma_{n-1},$$

von denen sogleich zu bemerken ist, dass sie arithmetische Invarianten der Form, nämlich für alle Formen einer Classe dieselben sind. Dies folgt bezüglich der Zahlen d_{m-1} bereits aus dem zweiten Capitel. Denn d_{m-1} bedeutet den grössten gemeinsamen Theiler der Determinanten m^{ten} Grades des Zahlensystems a, also dasselbe, was wir dort mit d_m bezeichnet haben, fortan aber aus Gründen der Symmetrie lieber d_{m-1} nennen wollen; für das Zahlensystem

$$b = q' \cdot a \cdot q$$

der äquivalenten Form muss deshalb d_{m-1} denselben Werth haben. Dasselbe ergiebt sich aus der Formel (70) vorigen Capitels, in welcher als besonderer Fall die folgende enthalten ist:

$$B^{(m)}_{hi\varkappa\cdots,\,hi\varkappa\cdots} = f^{(m)}(Q^{(m)}_{\varrho\sigma\tau\cdots,\,hi\varkappa\cdots}). \tag{3}$$

Denn, da die rechte Seite jener Formel eine homogene lineare Funktion der Coefficienten $A^{(m)}_{hi\varkappa\cdots,\,rst\cdots}$ ist, muss der grösste gemeinsame Theiler d_{m-1} der letzteren auch in sämmtlichen Coefficienten $B^{(m)}_{hi\varkappa\cdots,\,rst\cdots}$ aufgehen; und da bei äquivalenten Formen diese Beziehung umkehrbar ist, muss er dem grössten gemeinsamen Theiler der letzteren gleich sein. Da ferner wegen (51) vorigen Capitels die vorstehende Formel (3), sowie für verschiedene Combinationen $hi\varkappa\cdots$, $rst\cdots$ wenigstens die mit 2 multiplicirte Formel (70) jenes Capitels linear sind in den Zahlen

$$A^{(m)}_{hi\varkappa\cdots,\,hi\varkappa\cdots} \text{ und } 2\cdot A^{(m)}_{hi\varkappa\cdots,\,rst\cdots},$$

muss bei äquivalenten Formen auch der grösste gemeinsame Theiler der letzteren dem grössten gemeinsamen Theiler der Zahlen

$$B^{(m)}_{hi\varkappa\cdots,\,hi\varkappa\cdots} \text{ und } 2\cdot B^{(m)}_{hi\varkappa\cdots,\,rst\cdots}$$

gleich sein, w. z. b. w.

2. Neben den *bisherigen* Begleitformen führen wir nun andere *primitive* ein, indem wir setzen:

(4) $$\theta^{(m)}(x_{\varrho\sigma\tau}\ldots) = \frac{1}{d_{m-1}} \cdot f^{(m)}(x_{\varrho\sigma\tau}\ldots);$$

jenachdem $\sigma_m = 1$ oder $= 2$ ist, ist $\theta^{(m)}$ eine ungerade oder eine gerade Form, und umgekehrt. Ausserdem setzen wir

(5) $$o_1 = d_1 \text{ und } o_m = \frac{d_m}{d_{m-1}} : \frac{d_{m-1}}{d_{m-2}}$$
$$(\text{für } m = 2, 3, \cdots n-1).$$

Durch diese Formeln sind, falls $d_0 = 1$ ist, die Zahlen $o_1, o_2, \cdots o_{n-1}$ vermittelst der Zahlen $d_1, d_2, \cdots d_{n-1}$, aber auch umgekehrt diese durch jene vollkommen bestimmt, nämlich:

(6) $$\begin{cases} d_1 = o_1 \\ d_2 = o_1^2 o_2 \\ d_3 = o_1^3 o_2^2 o_3 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ d_{n-1} = o_1^{n-1} o_2^{n-2} \cdots o_{n-2}^2 \cdot o_{n-1}. \end{cases}$$

Man darf daher die Invarianten d auch durch die Invarianten o ersetzen. Nach nr. 3 des zweiten Capitels sind diese letzteren gleichfalls ganze Zahlen, denn $\frac{d_{m-1}}{d_{m-2}}$ und $\frac{d_m}{d_{m-1}}$ sind zwei aufeinanderfolgende Elementartheiler des Zahlensystems a.

Alle primitiven Formen nun, welche denselben Trägheitsindex τ, dieselben o- und dieselben σ-Invarianten haben, sollen Formen derselben *Ordnung*

(7) $$O : \tau, \begin{matrix} o_1, o_2, \cdots o_{n-1} \\ \sigma_1, \sigma_2, \cdots \sigma_{n-1} \end{matrix}$$

genannt werden. Man sieht, dass Formen derselben Ordnung stets auch dieselbe Determinante haben, und sonach zerfallen die Formen derselben Determinante in eine — der letzten der Formeln (6) wegen — endliche Anzahl verschiedener Ordnungen, deren dann jede wieder nur eine endliche Anzahl von Classen enthalten kann.

Für ternäre Formen ($n = 3$) giebt es nur eine Begleitform, die Adjungirte; man findet die Determinante gleich

$$(-1)^{\tau} \cdot o_1^2 o_2,$$

und da $o_1 = d_1$ den grössten gemeinsamen Theiler aller Coefficienten der Adjungirten bedeutet, stimmt o_2 mit dem in dem ersten Abschnitte benutzten Zeichen Δ, o_1 — jenachdem es sich um bestimmte oder unbestimmte Formen handelt — mit Ω oder $-\Omega$ überein.

Für die primitive $n-1^{\text{te}}$ Begleitform von $f(x_\varrho)$ findet nachstehende Beziehung statt:

$$\theta^{(n-1)}(x_{\varrho\sigma\tau\ldots}) = \frac{1}{d_{n-2}} \cdot f^{(n-1)}(x_{\varrho\sigma\tau\ldots}) = \frac{1}{d_{n-2}} \cdot F(x_u).$$

Bezeichnet man diese primitive Form für einen Augenblick mit $\varphi(x_u)$ und bildet die zugehörigen Begleitformen, so findet man

$$\varphi^{(m)}(x_{\varrho\sigma\tau\ldots}) = \frac{1}{d_{n-2}^m} \cdot F^{(m)}(x_{\varrho\sigma\tau\ldots}).$$

Da nun nach (54) vorigen Capitels

$$F^{(m)}(x_{\varrho\sigma\tau\ldots}) = \Delta^{m-1} \cdot f^{(n-m)}(x'_{\varrho'\sigma'\ldots})$$

und d_{n-m-1} der grösste gemeinsame Theiler der Coefficienten von $f^{(n-m)}$ ist, wird der grösste gemeinsame Theiler d'_{m-1} aller Coefficienten in $\varphi^{(m)}$ durch die Formel

$$d'_{m-1} = \frac{d_{n-1}^{m-1} \cdot d_{n-m-1}}{d_{n-2}^m} \tag{8}$$

gegeben, sodass, wenn o'_m für die Formel φ dasselbe bedeutet, was o_m für die Form $f(x_\varrho)$, sich leicht die Beziehung

$$o'_m = o_{n-m} \tag{9}$$

herausstellt. Bezeichnet ferner $\Theta^{(m)}$ die primitive m^{te} Begleitform von φ, so findet sich

$$\Theta^{(m)}(x_{\varrho\sigma\tau\ldots}) = \frac{1}{d'_{m-1}} \cdot \varphi^{(m)}(x_{\varrho\sigma\tau\ldots})$$

$$= \frac{1}{d_{n-m-1}} \cdot f^{(n-m)}(x'_{\varrho'\sigma'\ldots}) = \theta^{(n-m)}(x'_{\varrho'\sigma'\ldots}),$$

sie ist also mit $\theta^{n-m}(x'_{\varrho'\sigma'\ldots})$ gleichzeitig gerade oder ungerade und die σ-Invariante beider Formen muss dieselbe sein:

$$\sigma'_m = \sigma_{n-m}. \tag{10}$$

Die Gleichheiten (9) und (10) bleiben offenbar bestehen, auch

wenn man an Stelle der Form φ die Form $(-1)^\tau \cdot \varphi$ wählt. Da ferner τ der Trägheitsindex von f, diese Form also algebraisch der folgenden:

$$-(x_1^2 + \cdots + x_\tau^2) + (x_{\tau+1}^2 + \cdots + x_n^2)$$

äquivalent ist, so ist es nach nr. (7) vorigen Capitels die Adjungirte F von f der Adjungirten der letzteren, die dieser bis auf den Faktor $(-1)^\tau$ gleich ist, und somit hat $(-1)^\tau \cdot F$ den gleichen Trägheitsindex wie f. Dies überträgt sich sogleich auf die Form $(-1)^\tau \cdot \varphi$. Setzen wir also

$$\mathfrak{f}(x_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} \mathfrak{a}_{\alpha\beta} x_\alpha x_\beta, \tag{11}$$

wo

$$\mathfrak{a}_{\alpha\beta} = (-1)^\tau \cdot \frac{A_{\alpha\beta}}{d_{n-2}} \tag{12}$$

ist, so erhalten wir in der Form $\mathfrak{f}(x_\varrho)$ eine primitive Form der Ordnung

$$\tau, \frac{o_{n-1},\ o_{n-2},\ \cdots\ o_2,\ o_1}{\sigma_{n-1},\ \sigma_{n-2},\ \cdots\ \sigma_2,\ \sigma_1}, \tag{13}$$

deren primitive Begleitformen zugleich im wesentlichen die primitiven Begleitformen von f in umgekehrter Reihenfolge sind. W e g e n d i e s e r e i g e n t h ü m l i c h e n R e c i p r o c i t ä t, w e l c h e z w i s c h e n d e n F o r m e n f u n d $\mathfrak{f}$ b e s t e h t, w o l l e n w i r $\mathfrak{f}$ d i e R e c i p r o k e v o n f n e n n e n. O f f e n b a r i s t d a n n w i e d e r f d i e R e c i p r o k e v o n $\mathfrak{f}$. Wir bezeichnen noch mit $\mathbf{f}$ die Form $\mathfrak{f}$, wenn deren Unbestimmten in umgekehrter Reihenfolge gesetzt werden, sodass also

$$\mathbf{f}(x_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} \mathfrak{a}_{\alpha\beta} \cdot x_{n-\alpha+1} \cdot x_{n-\beta+1} \tag{14}$$

ist.

Ist $g(y_\varrho)$ eine zweite Form, $\mathfrak{g}(y_\varrho)$ ihre Reciproke und $\mathbf{g}(y_\varrho)$ die letztere bei umgekehrter Reihenfolge der Unbestimmten, so leuchtet ein, dass gleichzeitig mit $f(x_\varrho)$ und $g(y_\varrho)$ auch die Formen $\mathfrak{f}(x_\varrho)$ und $\mathfrak{g}(y_\varrho)$, sowie auch $\mathbf{f}(x_\varrho)$ und $\mathbf{g}(y_\varrho)$ einander äquivalent sein werden.

3. Die Classen einer Ordnung lassen sich in kleinere Gruppen vertheilen, welche G e s c h l e c h t e r heissen. Um zu

zeigen, worauf diese Vertheilung sich gründet, müssen wir eine Reihe von Congruenzbeziehungen ableiten, analog denjenigen von Smith, welche wir im dritten Capitel des ersten Abschnitts der Betrachtung zu Grunde gelegt haben. Wir bezeichnen dabei eine Form

$$\sum_{(\alpha,\beta=1,2,\cdots n)} a_{\alpha\beta}\, x_\alpha\, x_\beta$$

kurz durch $\{ a_{\alpha\beta} \}$ oder, ausführlicher dargestellt, durch das Schema ihrer n^2 Coefficienten:

$$\left\{ \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{matrix} \right\}$$

und nennen zwei Formen $\{ a'_{\alpha\beta} \}$ und $\{ a_{\alpha\beta} \}$ nach dem Modulus N congruent, in Zeichen:

$$\{ a'_{\alpha\beta} \} \equiv \{ a_{\alpha\beta} \} \pmod{N},$$

wenn für alle Werthe der Indices α, β

$$a'_{\alpha\beta} \equiv a_{\alpha\beta} \pmod{N}$$

ist; auch wird dann jede dieser Formen der Rest der anderen (mod. N) genannt.

Sei nun

$$f(x_\varrho) = \sum_{(\alpha,\beta=1,2,\cdots n)} a_{\alpha\beta}\, x_\alpha\, x_\beta$$

eine Form der Ordnung O. Ferner sei q irgend eine Primzahl und

$$q^{\partial_0},\ q^{\partial_1},\ \cdots\ q^{\partial_{n-1}}$$

die höchsten Potenzen derselben, welche resp. in

$$d_0,\ d_1,\ \cdots\ d_{n-1}$$

aufgehen. Wir nehmen $f(x_\varrho)$ prim gegen q an, sodass $\partial_0 = 0$ wird, und setzen

$$(15)\qquad \left\{ \begin{array}{c} \omega_1 = \partial_1 \\ \omega_m = \partial_m - \partial_{m-1} - (\partial_{m-1} - \partial_{m-2}); \\ (\text{für } m = 2, 3, \cdots n-1) \end{array} \right.$$

dann wird

$$(16)\qquad \omega_1 + \omega_2 + \cdots + \omega_m = \partial_m - \partial_{m-1}$$

und folglich

(17) $$m\omega_1 + (m-1)\omega_2 + \cdots + 2\omega_{m-1} + \omega_m = \delta_m.$$

Offenbar bedeutet ω_m den Exponenten der höchsten Potenz von q, welche in der ganzen Zahl o_m aufgeht, also eine nicht-negative ganze Zahl, und somit ist nicht nur wegen Gleichung (16)

(18) $$\partial_m \geqq \partial_{m-1} \quad (m = 1, 2, 3, \cdots n-1)$$

sondern auch wegen (15)

(19) $$\partial_m - \partial_{m-1} \geqq \partial_{m-1} - \partial_{m-2}. \quad (m = 2, 3, \cdots n-1)$$

Zunächst sei q eine ungerade Primzahl p. Da $f(x_\varrho)$ prim gegen p vorausgesetzt ist, giebt es eine eigentlich, d. h. mittels solcher Werthe der Unbestimmten, die keinen gemeinsamen Theiler haben, durch sie darstellbare ganze Zahl α, welche nicht durch p theilbar ist (s. nr. 1). Geschieht diese Darstellung durch die Werthe

$$q_{11},\; q_{21},\; \cdots\; q_{n1}$$

der Unbestimmten, so lassen sich (nach nr. 5 des dritten Capitels) $n(n-1)$ andere ganze Zahlen

$$q_{\alpha\beta} \;(\alpha = 1, 2, \cdots n;\; \beta = 2, 3, \cdots n)$$

so bestimmen, dass die Determinante $|q_{\alpha\beta}| = 1$ ist. Alsdann geht $f(x_\varrho)$ durch die Substitution

$$x_\alpha = q_{\alpha 1} y_1 + q_{\alpha 2} y_2 + \cdots + q_{\alpha n} y_n \quad (\alpha = 1, 2, \cdots n)$$

in eine äquivalente Form

$$\varphi(y_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} b_{\alpha\beta}\, y_\alpha\, y_\beta$$

über, deren erster Coefficient $b_{11} = \alpha$ ist. Auf diese Form wende man weiter die unimodulare Substitution

$$y_1 = z_1 + \beta_2 z_2 + \cdots + \beta_n z_n$$
$$y_\alpha = z_\alpha \text{ (für } \alpha = 2, 3 \cdots n)$$

an; in der entstehenden äquivalenten Form

$$\psi(z_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} c_{\alpha\beta}\, z_\alpha\, z_\beta$$

ist

$$c_{11} = b_{11} = \alpha$$

und (für $\varkappa > 1$)

$$c_{1\varkappa} = b_{1\varkappa} + 2b_{11} \cdot \beta_\varkappa,$$

durch passende Wahl der ganzen Zahlen $\beta_2, \beta_3, \cdots \beta_n$ kann also bewirkt werden, dass (für $\varkappa > 1$)

$$(20) \qquad c_{1\varkappa} \equiv 0 \pmod{p^t}$$

werde, wo t ein beliebig gewählter Exponent ist. Diese, mit f äquivalente Form ψ leistet also einer Congruenz Genüge von folgender Gestalt:

$$(21) \qquad \psi \equiv \left\{\begin{array}{l} \alpha, 0, \ 0, \ \cdots 0 \\ 0, c_{22}, c_{23}, \cdots c_{2n} \\ 0, c_{32}, c_{33}, \cdots c_{3n} \\ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \\ 0, c_{n2}, c_{n3}, \cdots c_{nn} \end{array}\right\} \pmod{p^t}.$$

Nun ist die Determinante $C = | c_{\alpha\beta} |$ der Form ψ gleich derjenigen der Form f, gleicherweise der grösste gemeinsame Theiler aller Unterdeterminanten m^{ten} Grades $C^{(m)}$ gleich demjenigen aller Unterdeterminanten $A^{(m)}$ desselben Grades, also gleich d_{m-1}, und $p^{\partial_{m-1}}$ die höchste in allen jenen aufgehende Potenz von p; andererseits sind jene den entsprechenden Unterdeterminanten des zur Rechten von (21) stehenden Schema, d. i., wenn man mit C' die Determinante der $(n-1)^2$ Zahlen

$$c_{\alpha\beta} \text{ (für } \alpha, \beta = 2, 3, \cdots n)$$

bezeichnet, einem der folgenden Ausdrücke:

$$\alpha \cdot C'^{(m-1)}, \ C'^{(m)} \text{ oder } 0$$

(mod. p^t) congruent. Wird demnach t grösser gedacht, als alle Zahlen ∂_{m-1}, so sieht man, dass $p^{\partial_{m-1}}$ die höchste Potenz von p ist, durch welche alle jene Ausdrücke theilbar sind. Für $m = 2$ insbesondere folgt hieraus und weil α prim ist gegen p, dass alle $c_{\alpha\beta}$ des Schema durch $p^{\partial_1} = p^{\omega_1}$ theilbar sind:

$$c_{\alpha\beta} = p^{\omega_1} \cdot a'_{\alpha\beta}.$$

Man gelangt also zu folgendem Satze:

Jede gegen p prime Form f ist einer anderen Form ψ äquivalent, für welche in Bezug auf eine hin-

reichend hohe Potenz von p als Modulus eine Congruenz besteht von folgender Gestalt:

$$(22) \qquad \psi \equiv \begin{Bmatrix} \alpha, 0, & \cdots 0 \\ 0, p^{\omega_1} a'_{22} & \cdots p^{\omega_1} a'_{2n} \\ 0, p^{\omega_1} a'_{32} & \cdots p^{\omega_1} a'_{3n} \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ 0, p^{\omega_1} a'_{n2} & \cdots p^{\omega_1} a'_{nn} \end{Bmatrix} \pmod{p^t},$$

während α durch p nicht theilbar ist.

Zugleich aber können nicht mehr sämmtliche $a'_{\alpha\beta}$ durch p theilbar sein, die Form $\{a'_{\alpha\beta}\}$ mit $n-1$ Unbestimmten ist demnach prim gegen p; und, wenn man $A' = | a'_{\alpha\beta} |$ setzt, so ist $p^{\partial_{m-1}}$ die höchste in den sämmtlichen Ausdrücken

$$\alpha \cdot p^{(m-1)\omega_1} \cdot A'^{(m-1)}, \; p^{m\omega_1} \cdot A'^{(m)}$$

aufgehende Potenz von p. Heissen also die zur Form $\{a'_{\alpha\beta}\}$ gehörigen, den ∂ und ω entsprechenden Zahlen ∂' und ω' resp. sodass die höchsten Potenzen von p, welche in allen $A'^{(m-1)}$ resp. $A'^{(m)}$ aufgehen, $p^{\partial'_{m-2}}$ resp. $p^{\partial'_{m-1}}$ sind, so folgt aus der voraufgehenden Betrachtung, dass ∂_{m-1} dem kleinsten der beiden Exponenten

$$(m-1)\omega_1 + \partial'_{m-2}, \; m\omega_1 + \partial'_{m-1}$$

gleich sein muss. Demnach findet sich, da analog mit (18)

$$\partial'_{m-1} \geqq \partial'_{m-2}$$

ist,

$$(23) \qquad \partial_{m-1} = (m-1)\omega_1 + \partial'_{m-2},$$

eine Beziehung, aus welcher nach (15) und der analogen auf die Zahlen ω' bezüglichen Formel ferner

$$(24) \qquad \omega_m = \omega'_{m-1}$$

hervorgeht.

Jetzt wiederholen wir dieselben Betrachtungen, indem wir auf die Form

$$\psi = \alpha z_1^2 + 2c_{12} z_1 z_2 + \cdots + 2c_{1n} z_1 z_n + p^{\omega_1} \cdot X,$$

in welcher

$$c_{12}, c_{13}, \cdots c_{1n} \equiv 0 \pmod{p^t},$$

$$X \equiv \sum_{(\alpha, \beta = 2, 3, \cdots n)} a'_{\alpha\beta} z_\alpha z_\beta \pmod{p^{t-\omega_1}}$$

ist, die Substitution anwenden:

$$z_1 = u_1$$
$$z_\alpha = q'_{\alpha 2} u_2 + q'_{\alpha 3} u_3 + \cdots + q'_{\alpha n} u_n$$
$$(\text{für } \alpha = 2, 3, \cdots n).$$

Wird die Determinante $|q'_{\alpha\beta}| = 1$ vorausgesetzt, so geht ψ in eine äquivalente Form ψ' über, in welcher der erste Coefficient ungeändert a ist, während $c_{1\alpha}$ in

$$c_{12} \cdot q'_{2\alpha} + c_{13} \cdot q'_{3\alpha} + \cdots + c_{1n} \cdot q'_{n\alpha}$$

übergeht, also $\equiv 0 \pmod{p^t}$ bleibt, die $q'_{\alpha\beta}$ aber so gewählt werden können, dass die Form X sich in eine andere X' verwandelt, welche der Congruenz

$$X' \equiv \begin{Bmatrix} \alpha', & 0, & & \cdots & 0 \\ 0, & p^{\omega_1'} \cdot a''_{33} & & \cdots & p^{\omega_1'} \cdot a''_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & p^{\omega_1'} \cdot a''_{n3} & & \cdots & p^{\omega_1'} \cdot a''_{nn} \end{Bmatrix} \pmod{p^{t-\omega_1}}$$

genügt, wo α' und die Form $\{a''_{\alpha\beta}\}$ prim sind gegen p. Da nach (24) $\omega_1' = \omega_2$ ist, findet sich nunmehr für die mit f äquivalente Form ψ' die Congruenz:

$$\psi' \equiv \begin{Bmatrix} \alpha, & 0, & 0 & \cdots & 0 \\ 0, & p^{\omega_1}\alpha', & 0 & \cdots & 0 \\ 0, & 0, & p^{\omega_1+\omega_2} a''_{33} & \cdots & p^{\omega_1+\omega_2} a''_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & p^{\omega_1+\omega_2} a''_{n3} & \cdots & p^{\omega_1+\omega_2} a''_{nn} \end{Bmatrix} \pmod{p^t}.$$

So fortfahrend gelangt man offenbar zu folgendem Satze:

Die gegen p prime Form f ist einer anderen Form f' äquivalent, für welche die Congruenz

$$(25) \quad f' \equiv \begin{Bmatrix} \alpha, & 0, & 0 & \cdots & 0 \\ 0, & p^{\omega_1}\alpha', & 0 & \cdots & 0 \\ 0, & 0, & p^{\omega_1+\omega_2} \cdot \alpha'' & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 0 & \cdots & p^{\omega_1+\omega_2+\cdots+\omega_{n-1}} \cdot \alpha^{(n-1)} \end{Bmatrix}$$

$\pmod{p^t}$ besteht, während

$$\alpha, \alpha', \alpha'', \cdots \alpha^{(n-1)}$$

prim sind gegen p. Es ist zu bemerken, dass, da einerseits die Congruenz, wenn (mod. p^t), so auch nach jeder geringeren Potenz von p als Modulus besteht, andererseits p^t oberhalb der bezeichneten Grenze als beliebig hohe Potenz gedacht werden darf, der ausgesprochene Satz zuletzt mit Bezug auf jede beliebig hohe Potenz von p ausgesagt werden darf.

4. Wir behandeln nun den noch übrigen Fall, wo $q = 2$ ist. Die Form f wird prim gegen 2 vorausgesetzt.

Ist erstens $\sigma_1 = 1$ d. i. f eine ungerade Form, so muss wenigstens einer ihrer Hauptcoefficienten $a_{11}, a_{22}, \cdots a_{nn}$ ungerade sein. Ist zudem $\omega_1 = \partial_1 = 0$ d. i. $d_1 = o_1$ ungerade, so muss auch wenigstens eine der Unterdeterminanten zweiten Grades ungerade sein, und zwar eine der Hauptunterdeterminanten dieses Grades, denn man überzeugt sich leicht, dass, wenn alle diese gerade wären, überhaupt sämmtliche Unterdeterminanten zweiten Grades es sein würden. Gesetzt also, $a_{hh}a_{kk} - a_{hk}^2$ wäre ungerade; entweder ist es dann auch einer der Coefficienten a_{hh}, a_{kk}. Im entgegengesetzten Falle muss etwa a_{ii} ungerade sein und dann ist möglicherweise es auch $a_{ii}a_{hh} - a_{ih}^2$. Andernfalls geht f durch die Substitution

$$x_k = x_i' + x_k'$$

in eine äquivalente Form über, in welcher die Grössen

$$a_{ii},\ a_{ii}a_{hh} - a_{ih}^2$$

resp. durch die folgenden:

$$a_{ii} + 2a_{ik} + a_{kk}$$
$$a_{ii}a_{hh} - a_{ih}^2 + 2(a_{ik}a_{hh} - a_{ih}a_{kh}) + a_{hh}a_{kk} - a_{kh}^2$$

ersetzt sind, und diese beiden sind ungerade. Immer also giebt es, sei es unmittelbar in der Form f, sei es in einer Transformirten, einen ungeraden Hauptcoefficienten, der im Falle $\omega_1 = 0$ in einer ungeraden Hauptunterdeterminante zweiten Grades auftritt. Durch eine blosse Vertauschung zweier Variabeln mit eventueller Aenderung ihres Vorzeichens kann man endlich erreichen, dass die Form f durch eine äquivalente Form

$$\varphi(y_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} b_{\alpha\beta}\, y_\alpha y_\beta$$

28*

ersetzt wird, in welcher jener Hauptcoefficient der erste geworden, also b_{11} eine ungerade Zahl α und zugleich, falls $\omega_1 = 0$ ist, etwa $b_{11}b_{hh} - b_{1h}^2$ ungerade ist. Diese Form verwandelt sich durch die Substitution

$$y_1 = z_1 + \beta_2 z_2 + \cdots + \beta_n z_n$$
$$y_\alpha = z_\alpha \text{ (für } \alpha = 2, 3, \cdots n)$$

in eine äquivalente Form

$$\psi(z_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} c_{\alpha\beta} z_\alpha z_\beta,$$

in welcher

$$c_{11} = b_{11}, \; c_{11}c_{hh} - c_{1h}^2 = b_{11}b_{hh} - b_{1h}^2$$

also im Falle $\omega_1 = 0$ ungerade sind, und welche bei passender Wahl der $\beta_2 \cdots \beta_n$ der Congruenz

$$\psi \equiv \begin{Bmatrix} \alpha, & 0, & 0 & \cdots & 0 \\ 0, & c_{22}, & c_{23}, & \cdots & c_{2n} \\ 0, & c_{32}, & c_{33}, & \cdots & c_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & c_{n2}, & c_{n3}, & \cdots & c_{nn} \end{Bmatrix} \pmod{2^t}$$

Genüge leistet. Man schliesst hieraus weiter bei gleicher Behandlungsweise wie vorher die Beziehungen

$$\partial_{m-1} = (m-1)\omega_1 + \partial'_{m-2} \tag{26}$$

$$\omega_m = \omega'_{m-1} \tag{27}$$

sowie auch die Congruenz:

$$\psi \equiv \begin{Bmatrix} \alpha, & 0, & 0 & \cdots & 0 \\ 0, & 2^{\omega_1} a'_{22}, & 2^{\omega_1} a'_{23} & \cdots & 2^{\omega_1} a'_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 2^{\omega_1} a'_{n2}, & 2^{\omega_1} a'_{n3} & \cdots & 2^{\omega_1} a'_{nn} \end{Bmatrix} \pmod{2^t}, \tag{28}$$

wo nun $\{a'_{\alpha\beta}\}$ eine gegen 2 prime quadratische Form mit nur $n-1$ Unbestimmten ist*).

---

*) Da bis hierher von der, die Unterdeterminanten zweiten Grades betreffenden Voraussetzung kein Gebrauch gemacht worden ist, sieht man leicht ein, dass die vorstehende Congruenz auch für jeden ungeraden Werth α hergeleitet werden kann, der durch f darstellbar ist, denn es giebt dann eine mit f äquivalente Form φ, deren erster Coefficient α ist.

Man bemerke aber im gegenwärtigen Falle, dass die symmetrischen Unterdeterminanten $C^{(m)}_{hik\dots,hik\dots}$ und die doppelt genommenen unsymmetrischen $2C^{(m)}_{hik\dots,rst\dots}$ den grössten gemeinsamen Theiler $\sigma_m d_{m-1}$ haben, dass also ihre höchste gemeinsame Potenz von 2 gleich $\sigma_m \cdot 2^{\partial_{m-1}}$ ist. Nach (28) sind sie (mod. 2^t) einem der folgenden Ausdrücke:

$$\alpha \cdot 2^{(m-1)\omega_1} \cdot A'^{(m-1)}_{hik\dots,hik\dots},\quad 2^{m\omega_1} \cdot A'^{(m)}_{hik\dots,hik\dots}$$
$$\alpha \cdot 2^{(m-1)\omega_1} \cdot 2A'^{(m-1)}_{hik\dots,rst\dots},\quad 2^{m\omega_1} \cdot 2A'^{(m)}_{hik\dots,rst\dots},\quad 0$$

congruent; wird demnach $2^t > \sigma_m \cdot 2^{\partial_m - 1}$ gedacht, so ergiebt sich hieraus $\sigma_m \cdot 2^{\partial_m - 1}$ gleich der kleineren der folgenden Potenzen:

(29) $$\sigma'_{m-1} \cdot 2^{(m-1)\omega_1 + \partial'_m - 2} \text{ und } \sigma'_m \cdot 2^{m\omega_1 + \partial'_m - 1}.$$

Wenn $\omega_1 > 0$ ist, ist jedenfalls die erste derselben nicht grösser als die zweite. Somit kommt in diesem Falle

$$\sigma_m \cdot 2^{\partial_m - 1} = \sigma'_{m-1} \cdot 2^{(m-1)\omega_1 + \partial'_m - 2}$$

d. i. mit Rücksicht auf (26)

(30) $$\sigma_m = \sigma'_{m-1};$$

insbesondere ergiebt sich

(30a) $$\sigma_2 = \sigma_1'.$$

Wenn aber $\omega_1 = 0$ ist, so ist $\sigma_2 = 1$, da in ψ eine der Hauptunterdeterminanten zweiten Grades ungerade ist; aus (28) schliesst man ferner, dass $\alpha \cdot 2^{\omega_1} a'_{hh} = \alpha \cdot a'_{hh}$ also auch a'_{hh} ungerade und somit $\sigma_1' = 1$ ist; es besteht also auch in diesem Falle die Gleichung (30a). Man kann aber die Form $\{a'_{\alpha\beta}\}$ einer ähnlichen Transformation unterwerfen, wie die Form f, bei welcher die Congruenz (28), wie man sich leicht überzeugt, ihre charakteristische Gestalt nicht verändert, und kann also in dem besonderen Falle, wo $\omega_1' = \omega_2 = 0$ d. i. o_2 ungerade ist, noch wieder in gleicher Weise fortschliessen, und so endlich, wenn alle ω gleich Null oder alle Invarianten o_1, $o_2, \cdots o_{n-1}$ ungerade sind d. i. im Falle einer ungeraden Determinante folgenden Satz aussprechen:

Eine gegen 2 prime ungerade Form f mit ungerader Determinante ist stets einer Form f' äquivalent, für welche, während

$$\alpha, \alpha', \alpha'', \cdots \alpha^{(n-1)}$$

ungerade Zahlen sind, die Congruenz besteht:

$$(31) \qquad f' \equiv \begin{Bmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & \alpha' & 0 & \cdots & 0 \\ 0 & 0 & \alpha'' & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & \alpha^{(n-1)} \end{Bmatrix} \pmod{2^t}.$$

Hieraus geht hervor, dass ihre sämmtlichen σ-Invarianten gleich 1 sind.

Nun war $\sigma_m \cdot 2^{\partial_m - 1}$ die kleinere der beiden Potenzen (29) d. h. im vorliegenden Falle die kleinere der Potenzen

$$\sigma'_{m-1} \cdot 2^{\partial'_m - 2}$$

und

$$\sigma'_m \cdot 2^{\partial'_m - 1} = \sigma'_m \cdot 2^{\partial_m - 2 + \omega'_1 + \omega'_2 + \cdots + \omega'_{m-1}}.$$

Im vorliegenden Falle sind aber sämmtliche Invarianten ω, demnach auch sämmtliche ω' gleich Null; da zudem $\sigma_1' = 1$ ist, so sind dem eben bewiesenen Satze zufolge die sämmtlichen Invarianten σ' der Form $\{a'_{\alpha\beta}\}$ gleich 1; alsdann ist aber die erste jener Potenzen nicht grösser als die zweite. Somit ist die Formel (30) auch für den Fall erwiesen, wo ω_1, zugleich aber auch die übrigen ω gleich Null sind.

5. Sei jetzt zweitens $\sigma_1 = 2$. In diesem Falle lässt sich durch f das Doppelte einer ungeraden Zahl eigentlich darstellen und demnach f sich in eine äquivalente Form

$$(32) \qquad \sum_{(\alpha, \beta = 1, 2, \cdots n)} b_{\alpha\beta} y_\alpha y_\beta$$

verwandeln, in der mindestens einer der Hauptcoefficienten $\equiv 2 \pmod{4}$ ist.

Wegen $\sigma_1 = 2$ müssen sämmtliche ihrer Hauptcoefficienten gerade, mindestens einer der übrigen Coefficienten $b_{\alpha\beta}$ aber ungerade sein. Angenommen also, b_{hk} sei ungerade; entweder ist dann einer der Coefficienten b_{hh}, $b_{kk} \equiv 2 \pmod{4}$. Im entgegengesetzten Falle muss etwa $b_{ii} \equiv 2 \pmod{4}$ sein; wäre aber dann keine der Zahlen b_{ih}, b_{ik} ungerade, so ginge die Form (32) durch die Substitution $x_k = x_i' + x_k'$ in eine äqui-

valente Form über, in welcher die Coefficienten b_{ii}, b_{ik} durch die folgenden:

$$b_{ii} + 2b_{ik} + b_{kk}, \; b_{ik} + b_{kk}$$

ersetzt sind, von denen der erste $\equiv 2 \pmod{4}$, der zweite ungerade ist. Immer also kann man f durch eine äquivalente Form ersetzen, in welcher das Quadrat einer Variabeln und zugleich eines derjenigen Produkte zweier Veränderlichen, welche dieselbe Variable enthalten, in das Doppelte einer ungeraden Zahl multiplicirt sind. Durch blosse Vertauschung der Variabeln endlich wird f äquivalent mit einer Form von folgender Gestalt:

$$\varphi(y_\varrho) = 2\alpha y_1^2 + 2\beta y_2^2 + 2b_{12}y_1y_2 + 2 \cdot \sum_{i=3}^{n} (b_{1i}y_1 + b_{2i}y_2)y_i + \cdots,$$

worin α, b_{12} ungerade sind und die fortgelassenen Glieder nur solche y enthalten, deren Index grösser als 2 ist. Durch die Substitution

$$(33) \quad \begin{cases} y_1 = z_1 + \delta z_2 + \beta_3 z_3 + \cdots + \beta_n z_n \\ y_2 = z_2 + \gamma_3 z_3 + \cdots + \gamma_n z_n \\ y_\alpha = z_\alpha \; (\text{für } \alpha = 3, 4, \cdots n) \end{cases}$$

verwandelt sich $\varphi(y_\varrho)$ in eine äquivalente Form $\psi(z_\varrho)$ von folgender Gestalt:

$$\psi(z_\varrho) = 2\alpha z_1^2 + 2\mathfrak{a} z_2^2 + 2\mathfrak{B}_{12}z_1z_2 + 2\sum_{i=3}^{n} (\mathfrak{B}_{1i} \cdot z_1 + \mathfrak{B}_{2i} \cdot z_2)z_i + \cdots,$$

in welcher

$$\mathfrak{B}_{12} = 2\alpha \cdot \delta + b_{12}$$
$$\mathfrak{B}_{1i} = 2\alpha \cdot \beta_i + b_{12} \cdot \gamma_i + b_{1i}$$
$$\mathfrak{B}_{2i} = \delta \mathfrak{B}_{1i} + b_{12} \cdot \beta_i + 2\beta \cdot \gamma_i + b_{2i}$$

ist. Da aber α und ebenfalls $4\alpha\beta - b_{12}^2$ ungerade ist, so gestattet sowohl die Congruenz

$$2\alpha \cdot \delta + b_{12} \equiv \mathfrak{A} \pmod{2^\ell},$$

wenn man unter $\mathfrak{A}$ eine beliebige ungerade Zahl versteht, als auch für jedes i das System der zwei Congruenzen

$$\left.\begin{array}{l} 2\alpha \cdot \beta_i + b_{12} \cdot \gamma_i + b_{1i} \equiv 0 \\ b_{12} \cdot \beta_i + 2\beta \cdot \gamma_i + b_{2i} \equiv 0 \end{array}\right\} \pmod{2^t}$$

eine Auflösung; werden also die Coefficienten der Substitution (33) diesen Congruenzen gemäss gewählt, so erhält man für die Form ψ eine Congruenz von folgender Gestalt:

$$(34)\qquad \psi \equiv \left\{\begin{array}{lllll} 2\alpha, & \mathfrak{A}, & 0 & \cdots & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 & \cdots & 0 \\ 0, & 0, & c_{33} & \cdots & c_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & c_{n3} & \cdots & c_{nn} \end{array}\right\} \pmod{2^t},$$

in welcher $\mathfrak{A}$ eine beliebig gewählte ungerade Zahl und auch α ungerade ist. Nun bezeichne wieder C die Determinante von ψ und C' die Determinante $|c_{\alpha\beta}|$ für $\alpha, \beta = 3, 4, \cdots n$; dann haben die sämmtlichen Unterdeterminanten $C^{(m)}$ den grössten gemeinsamen Theiler d_{m-1}, nach der vorstehenden Congruenz aber sind sie (mod. 2^t) einem der folgenden Ausdrücke congruent:

$$(4\alpha\mathfrak{a} - \mathfrak{A}^2) \cdot C'^{(m-2)}$$
$$2\alpha \cdot C'^{(m-1)}, \quad \mathfrak{A} \cdot C'^{(m-1)}, \quad 2\mathfrak{a} \cdot C'^{(m-1)}$$
$$C'^{(m)} \text{ oder } 0,$$

und diese müssen folglich, wenn t grösser als jede der Zahlen ∂_{m-1} gewählt wird, $2^{\partial_{m-1}}$ zur höchsten gemeinsamen Potenz von 2 haben. Insbesondere lässt der erste dieser Ausdrücke wegen des ungeraden $4\alpha\mathfrak{a} - \mathfrak{A}^2$ erkennen,

$$\text{für } m = 2, \text{ dass } \partial_1 = \omega_1 = 0,$$
$$\text{für } m = 3, \text{ dass } c_{\alpha\beta} = 2^{\partial_2} \cdot a'_{\alpha\beta},$$

die Zahlen $a'_{\alpha\beta}$ aber nicht mehr sämmtlich gerade sind. Die Congruenz (34) nimmt mithin folgende Gestalt an:

$$(35)\qquad \psi \equiv \left\{\begin{array}{lllll} 2\alpha, & \mathfrak{A}, & 0 & & \cdots 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 & & \cdots 0 \\ 0, & 0, & 2^{\omega_2} \cdot a'_{33} & \cdots & 2^{\omega_2} \cdot a'_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 2^{\omega_2} \cdot a'_{n3} & \cdots & 2^{\omega_2} \cdot a'_{nn} \end{array}\right\} \pmod{2^t},$$

in welcher die Form $\{a'_{\alpha\beta}\}$ prim gegen 2 ist. Werden dann

die Determinante $|a'_{\alpha\beta}|$ der letzteren mit A' und mit ∂', ω' die dieser Form angehörigen mit den ∂, ω analogen Zahlen bezeichnet, so muss $2^{\partial_{m-1}}$ die niedrigste der folgenden Potenzen sein:

$$2^{(m-2)\omega_2+\partial'_{m-3}}$$

$$2^{(m-1)\omega_2+1+\partial'_{m-2}},\quad 2^{(m-1)\omega_2+\partial'_{m-2}},\quad 2^{(m-1)\omega_2+1+\partial'_{m-2}}$$

$$2^{m\omega_2+\partial'_{m-1}}.$$

Da nun analog mit (18)

$$\partial'_{m-1} \geqq \partial'_{m-2} \geqq \partial'_{m-3}$$

ist, findet sich hieraus

$$(36)\qquad \partial_{m-1} = (m-2)\omega_2 + \partial'_{m-3},$$

eine Formel, aus welcher leicht noch die andere:

$$(37)\qquad \omega_m = \omega'_{m-2}$$

erschlossen wird. — Aus der Congruenz (35) folgt weiter, dass die symmetrischen Unterdeterminanten m^{ten} Grades von ψ einem der folgenden Ausdrücke:

$$(4\alpha\mathfrak{a} - \mathfrak{A}^2)\cdot 2^{(m-2)\omega_2}\cdot A'^{(m-2)}_{hi\cdots,hi\cdots}$$

$$2\alpha\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,hi\cdots},\quad 2\mathfrak{a}\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,hi\cdots},$$

$$2^{m\omega_2}\cdot A'^{(m)}_{hik\cdots,hik\cdots},$$

dagegen die unsymmetrischen einem der folgenden:

$$(4\alpha\mathfrak{a} - \mathfrak{A}^2)\cdot 2^{(m-2)\omega_2}\cdot A'^{(m-2)}_{hi\cdots,rs\cdots}$$

$$2\alpha\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,rs\cdots},\quad 2\mathfrak{a}\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,rs\cdots},$$

$$2^{m\omega_2}\cdot A'^{(m)}_{hik\cdots,rst\cdots}$$

$$\mathfrak{A}\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,hi\cdots},\quad \mathfrak{A}\cdot 2^{(m-1)\omega_2}\cdot A'^{(m-1)}_{hi\cdots,rs\cdots},\quad 0$$

(mod. 2^{ι}) congruent sind. Demnach wird $\sigma_m\cdot 2^{\partial_{m-1}}$ der kleinsten der nachstehenden Potenzen:

$$(38)\qquad \begin{cases} \qquad\qquad \sigma'_{m-2}\cdot 2^{\partial'_{m-3}+(m-2)\omega_2} \\ \qquad\qquad \sigma'_{m-1}\cdot 2^{\partial'_{m-2}+(m-1)\omega_2} \\ = \sigma'_{m-1}\cdot 2^{\partial'_{m-3}+(m-2)\omega_2+\omega_2+\omega_1'+\cdots+\omega'_{m-2}} \\ \qquad\qquad \sigma'_{m}\cdot 2^{\partial'_{m-1}+m\omega_2} \\ = \sigma'_{m}\cdot 2^{\partial'_{m-2}+(m-1)\omega_2+\omega_2+\omega_1'+\cdots+\omega'_{m-1}} \end{cases}$$

gleich sein. Ist demnach eine der Zahlen

$$\omega_2,\ \omega_1' = \omega_3,\ \omega_2' = \omega_4,\ \cdots \omega_{m-2}' = \omega_m$$

von Null verschieden, so ist

$$\sigma_m \cdot 2^{\partial_m - 1} = \sigma_{m-2}' \cdot 2^{\partial_{m-3}' + (m-2)\omega_2}$$

d. i. mit Rücksicht auf (36)

$$\sigma_m = \sigma_{m-2}'. \tag{39}$$

Verfolgen wir diese Betrachtung unter der besonderen Voraussetzung, dass $\omega_2 = 0$ ist. Da ψ eine gerade Form, so müssen die sämmtlichen Coefficienten $2^{\omega_2} \cdot a_{\alpha\alpha}'$, in der gemachten Voraussetzung also sämmtliche Zahlen $a_{\alpha\alpha}'$ gerade sein; die Form $\{a_{\alpha\beta}'\}$ ist alsdann also eine gerade Form und ihre Invariante $\sigma_1' = 2$. Demnach lässt sich die voraufgehende Betrachtung nun für diese Form wiederholen, man findet

$$\partial_1' = \omega_1' = \omega_3 = 0$$

und könnte, falls $\omega_2' = \omega_4$ wieder Null wäre, noch einmal so fortfahren u. s. w. Dieser Fall wird sich dann, aber auch nur dann ereignen, wenn die Determinante ungerade und zugleich die Anzahl n der Unbestimmten gerade ist. In der That sind dann die sämmtlichen Invarianten o_m ungerade also sämmtliche $\omega_m = 0$; bei ungeradem n ist dieser Fall unmöglich, denn dann würde als letzte der neu eintretenden Formen die Form einer Variabeln

$$2^{\omega_{n-1}} \cdot az^2$$

eingeführt, in welcher einerseits der Coefficient a nicht mehr durch 2 theilbar wäre, andererseits aber $2^{\omega_{n-1}} \cdot a$, weil ψ eine gerade Form ist, gerade sein müsste, was für

$$\omega_{n-1} = 0$$

einen Widerspruch ergiebt. So gelangen wir endlich zu folgendem Resultate:

Eine zu 2 prime gerade Form f mit ungerader Determinante (und gerader Anzahl der Veränderlichen) ist stets einer Form f' äquivalent, für welche die Congruenz besteht:

$$(40)\quad f' \equiv \begin{Bmatrix} 2\alpha, & \mathfrak{A}, & 0, & 0, & \cdots 0, & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0, & 0, & \cdots 0, & 0 \\ 0, & 0, & 2\alpha', & \mathfrak{A}' & \cdots 0, & 0 \\ 0, & 0, & \mathfrak{A}', & 2\mathfrak{a}' & \cdots 0, & 0 \\ . & . & . & . & . & . \\ 0, & 0, & 0, & 0, & \cdots 2\alpha^{\left(\frac{n}{2}-1\right)}, & \mathfrak{A}^{\left(\frac{n}{2}-1\right)} \\ 0, & 0, & 0, & 0, & \cdots \mathfrak{A}^{\left(\frac{n}{2}-1\right)}, & 2\mathfrak{a}^{\left(\frac{n}{2}-1\right)} \end{Bmatrix}$$

(mod. 2^ϱ); darin sind

$$\alpha,\ \alpha',\ \cdots\ \alpha^{\left(\frac{n}{2}-1\right)}$$

bestimmte,

$$\mathfrak{A},\ \mathfrak{A}',\ \cdots\ \mathfrak{A}^{\left(\frac{n}{2}-1\right)}$$

beliebige ungerade Zahlen.

Man erkennt hieraus leicht, dass die σ-Invarianten der Form f folgende Werthe haben:

$$\sigma_1 = 2,\ \sigma_2 = 1,\ \sigma_3 = 2,\ \sigma_4 = 1,\ \cdots \sigma_{n-2} = 1,\ \sigma_{n-1} = 2.$$

Nun war $\sigma_m \cdot 2^{\partial_m - 1}$ die kleinste der Potenzen (38); aber im gegenwärtigen Falle sind ω_2 und sämmtliche Zahlen

$$\omega_1' = \omega_3,\ \omega_2' = \omega_4,\ \cdots \omega_{n-3}' = \omega_{n-1}$$

gleich Null, während zugleich $\sigma_1' = 2$ war. In Folge des letzten Satzes erhalten daher die σ'-Invarianten der Form $\{a'_{\alpha\beta}\}$ die Werthe

$$\sigma_1' = 2,\ \sigma_2' = 1,\ \sigma_3' = 2,\ \sigma_4' = 1,\ \cdots,$$

deren Vergleichung mit denjenigen der σ-Invarianten auch für diesen Fall die Gleichheit

$$(39)\qquad \sigma_m = \sigma_{m-2}'$$

ergiebt.

6. Ist die Determinante der Form f gerade, so bietet sich eine grössere Mannigfaltigkeit dar. Eine weitere Durchführung unserer Betrachtungen führt, wie Minkowski gezeigt hat*), zu einem allgemeinen Satze, dem wir noch

*) Minkowski, Mémoire sur la théorie des formes quadratiques à coefficiens entiers, in Mém. prés. p. div. Sav. Etrangers etc. t. 29.

einige Erklärungen voraufschicken: Wir setzen — gleichviel, ob sich die Zeichen ω auf eine ungerade Primzahl beziehen oder auf die Zwei —

$$v_m = \omega_1 + \omega_2 + \cdots + \omega_m, \tag{41}$$

sodass

$$\partial_m = v_1 + v_2 + \cdots + v_m \tag{42}$$

geschrieben werden darf; unter den Zahlen

$$\omega_1, \omega_2, \cdots \omega_{n-1}$$

aber bezeichnen wir der Reihe nach diejenigen, welche von Null verschieden sind, mit

$$\omega_{\vartheta_1}, \omega_{\vartheta_2}, \cdots \omega_{\vartheta_{\lambda-1}} \tag{43}$$

und führen neben den Zahlen $\vartheta_1, \vartheta_2, \cdots \vartheta_{\lambda-1}$ ebensoviel andere $\varkappa_1, \varkappa_2, \cdots \varkappa_{\lambda-1}$ durch folgende Gleichung ein:

$$\vartheta_m = \varkappa_1 + \varkappa_2 + \cdots + \varkappa_m. \tag{44}$$

Noch setzen wir

$$\vartheta_0 = 0, \ \vartheta_\lambda = n, \ v_{\vartheta_0} = 0. \tag{45}$$

Diesen Definitionen zufolge bestehen zunächst die Ungleichheiten:

$$0 = v_{\vartheta_0} < v_{\vartheta_1} < v_{\vartheta_2} \cdots < v_{\vartheta_{\lambda-1}}. \tag{46}$$

Der gedachte allgemeine Satz aber lautet, wie folgt:

Eine gegen 2 prime Form f ist stets einer anderen f' äquivalent, für welche bei hinreichend grossem ζ die Congruenz besteht:

$$f' \equiv \sum_{i=1}^{\lambda} 2^{v_{\vartheta_{i-1}}} \cdot \Phi_i \pmod{2^\zeta}, \tag{47}$$

während die Form Φ_i, wenn $\varkappa_i$ ungerade ist, die Gestalt

$$\Phi_i = \sum_{s=1}^{\varkappa_i} a_s^i \cdot \xi_s^i \xi_s^i, \tag{47a}$$

wenn aber $\varkappa_i$ gerade ist, entweder dieselbe oder auch die folgende Gestalt hat:

$$\Phi_i = \sum_{s=1}^{\frac{1}{2}\varkappa_i} (2a_s^i \xi_s^i \cdot \xi_s^i + 2\mathfrak{A}_s^i \cdot \xi_s^i \xi_s'^i + 2\mathfrak{a}_s^i \cdot \xi_s'^i \xi_s'^i). \tag{47b}$$

Die Formen (47a) wollen wir Formen der ersten, die Formen (47b) Formen der zweiten Art nennen. Was die Invarianten σ der Form f anbelangt, so haben sie, entsprechend den Werthen

$$m = \vartheta_{i-1} + 1, \; \vartheta_{i-1} + 2, \cdots \vartheta_i$$

entweder sämmtlich den Werth 1, wenn nämlich Φ_i von der ersten Art ist, oder abwechselnd die Werthe 2, 1, 2, 1, $\cdots$ 2, 1, wenn nämlich Φ_i von der zweiten Art ist; es ist mithin immer

$$\sigma_{\vartheta_i} = 1. \tag{48}$$

Wir setzen auch $\sigma_0 = 1$, $\sigma_n = 1$; die vorige Gleichung besteht dann für

$$i = 0, 1, 2, \cdots \lambda.$$

Aus diesen Umständen, welche die vorher abgeleiteten besonderen Fälle bestätigen, ziehen wir einige Folgerungen. Wir setzen dabei

$$2^{\mu_m} = \sigma_{m-1} \cdot 2^{\omega_m} \cdot \sigma_{m+1}. \tag{49}$$

Sei erstens $m = \vartheta_i (i = 1, 2, \cdots \lambda - 1)$, also $\sigma_m = 1$; man findet

$\mu_m = \omega_m$, wenn Φ_i, Φ_{i+1} von der ersten Art,

$\mu_m = \omega_m + 1$, wenn sie verschiedener Art,

$\mu_m = \omega_m + 2$, wenn sie beide von der zweiten Art sind.

Sei zweitens m zwischen ϑ_{i-1} und ϑ_i $(i = 1\, 2 \cdots \lambda)$; entweder ist dann Φ_i erster Art, also $\sigma_m = 1$ und jedenfalls auch $\sigma_{m-1} = 1$, aber auch $\sigma_{m+1} = 1$, da Φ_i aus mehr als einem Gliede bestehend zu denken ist; da $\omega_m = 0$ ist, ergiebt sich

$$\mu_m = 0.$$

Oder Φ_i ist zweiter Art; dann durchläuft σ_m, wenn m die angegebenen Werthe annimmt, abwechselnd die Werthe 2, 1, 2, 1, $\cdots$ 2, entsprechend ist σ_{m-1} abwechselnd 1, 2, $\cdots$ 1 und σ_{m+1} ebenfalls, während $\omega_m = 0$ bleibt. Also wird abwechselnd

$$\mu_m = 0, 2, 0, 2, \cdots 0$$

sein. Hieraus sieht man, dass, so oft $\sigma_m = 2$ ist, $\mu_m = 0$

und folglich

$$\sigma_{m-1} \cdot o_m \cdot \sigma_{m+1}$$

ungerade ist. Ferner aber folgt:

1) Der Fall $\mu_m = 0$ kommt nur vor, wenn Φ_i erster Art und m zwischen ϑ_{i-1} und ϑ_i ist, oder, wenn Φ_i zweiter Art und $m = \vartheta_{i-1} + 2m' - 1 < \vartheta_i$ ist;

2) Der Fall $\mu_m = 1$ kommt nur vor, wenn $m = \vartheta_i$ und zugleich $\omega_m = 1$ ist;

3) Der Fall $\mu_m \overline{\overline{>}} 2$ tritt nur ein, wenn entweder $m = \vartheta_i$ ist, oder, falls Φ_i zweiter Art ist, für $m = \vartheta_{i-1} + 2m' < \vartheta_i$;

4) Der Fall $\mu_m \overline{\overline{>}} 3$ nur in der ersten dieser Voraussetzungen.

5) Verbindet man die Voraussetzungen

$$\mu_m = 1, \; \mu_{m-1} \overline{\overline{>}} 2, \; \mu_{m+1} \overline{\overline{>}} 2,$$

so muss zunächst $m = \vartheta_i$ und $\omega_m = 1$ sein, zugleich aber, wie leicht zu übersehen,

$$m - 1 = \vartheta_{i-1}, \; m + 1 = \vartheta_{i+1},$$

sodass

$$\vartheta_{i+1} - \vartheta_i = \vartheta_i - \vartheta_{i-1} = 1$$

ist. Da hiernach Φ_i, Φ_{i+1} beide erster Art sind, muss $\omega_{\vartheta_{i+1}} > 1$ sein, wenn Φ_{i+2}, und $\omega_{\vartheta_{i-1}} > 1$ sein, wenn Φ_{i-1} erster Art ist.

6) Die gleichzeitigen Voraussetzungen

$$\mu_m = 0, \; \mu_{m-1} \overline{\overline{>}} 2, \; \mu_{m+1} \overline{\overline{>}} 2$$

erfordern, wenn Φ_i von zweiter Art ist,

$$m = \vartheta_{i-1} + 2m' - 1$$

also $\sigma_m = 2$; wird also zugleich $\sigma_m = 1$ vorausgesetzt, so muss Φ_i von erster Art sein und

$$m = \vartheta_{i-1} + m', \; m - 1 = \vartheta_{i-1} + m' - 1 = \vartheta_{i-1},$$
$$m + 1 = \vartheta_{i-1} + m' + 1 = \vartheta_i,$$
$$\text{d. h. } m = \vartheta_{i-1} + 1, \; \vartheta_i = \vartheta_{i-1} + 2;$$

und zwar muss $\omega_{\vartheta_{i-1}} > 1$ sein, wenn Φ_{i-1} erster Art ist, und ebenso $\omega_{\vartheta_i} > 1$, wenn Φ_{i+1} erster Art ist.

7. Wir bezeichnen nunmehr mit N eine ganze Zahl, deren Primzahlpotenzen $2^{t_0}, p^t, p'^{t'}, \cdots$ hinreichend hoch sind, um

die Sätze (25) bezw. (40) oder (47) zur Anwendung bringen zu können. Ist also $f = \{a_{i\varkappa}\}$ eine gegen N prime Form von n Veränderlichen, was jedenfalls zutrifft, so oft f eine primitive Form ist, so giebt es mit $\{a_{i\varkappa}\}$ äquivalente Formen $\{\alpha_{i\varkappa}\}$, $\{\beta_{i\varkappa}\}$, $\{\beta'_{i\varkappa}\}, \cdots$, welche resp. der Congruenz (47), (25) und den mit der letzteren analogen Congruenzen nach den Moduln $2^{t_0}, p^t, p'^{t'}, \cdots$ Genüge leisten, Congruenzen, die wir kurz durch die nachstehenden andeuten wollen:

$$(50) \qquad \{\alpha_{i\varkappa}\} \equiv \{\lambda_{i\varkappa}\} \pmod{2^{t_0}}, \quad \{\beta_{i\varkappa}\} \equiv \{\mu_{i\varkappa}\} \pmod{p^t} \cdots$$

und, wenn wir die n^2 Zahlen $n_{i\varkappa}$, was möglich ist, so wählen, dass

$$n_{i\varkappa} \equiv \lambda_{i\varkappa} \pmod{2^{t_0}}, \quad n_{i\varkappa} \equiv \mu_{i\varkappa} \pmod{p^t}, \cdots$$

ist, auch durch die anderen:

$$(51) \qquad \{\alpha_{i\varkappa}\} \equiv \{n_{i\varkappa}\} \pmod{2^{t_0}}, \quad \{\beta_{i\varkappa}\} \equiv \{n_{i\varkappa}\} \pmod{p^t}, \cdots$$

ersetzen können. Sind $(\mathfrak{a}_{i\varkappa})$, $(\mathfrak{b}_{i\varkappa})$, $(\mathfrak{b}'_{i\varkappa}) \cdots$ die Substitutionen, durch welche f in diese äquivalenten Formen übergeht, oder auch die aus ihren Coefficienten gebildeten Zahlensysteme, so ist, mit Beibehaltung der in Cap. 1 nr. 3 eingeführten Bezeichnungsweise und nach (22) vorigen Capitels

$$(\mathfrak{a}_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (\mathfrak{a}_{i\varkappa}) = (\alpha_{i\varkappa}), \quad (\mathfrak{b}_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (\mathfrak{b}_{i\varkappa}) = (\beta_{i\varkappa}), \cdots.$$

Nun sind die Substitutionen unimodular; jedes System $(c_{i\varkappa})$ also, welches den Congruenzen

$$(52) \qquad c_{i\varkappa} \equiv \mathfrak{a}_{i\varkappa} \pmod{2^{t_0}}, \quad c_{i\varkappa} \equiv \mathfrak{b}_{i\varkappa} \pmod{p^t}, \cdots$$

genügt, wird einen Modulus haben, der nach jedem der Moduln $2^{t_0}, p^t, p'^{t'} \cdots$ also auch (mod. N) congruent 1 ist:

$$(53) \qquad |c_{i\varkappa}| \equiv 1 \pmod{N};$$

und jedes, mit einem solchen Zahlensysteme (mod. N) congruente Zahlensystem $(c_{i\varkappa})$ wird nicht nur den Congruenzen (52), sondern auch der Congruenz (53) genügen, und unter diesen Systemen kann eines nach der am Schlusse des vorigen Capitels auseinandergesetzten Methode so gewählt werden, dass letztere Congruenz durch die Gleichheit

$$|c_{i\varkappa}| = 1$$

ersetzt wird. Schreibt man dann

$$(c_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (c_{i\varkappa}) = (a'_{i\varkappa}),$$

so ist offenbar

$$\{a'_{i\varkappa}\} \equiv \{\alpha_{i\varkappa}\} \equiv \{n_{i\varkappa}\} \pmod{2^{t_0}}$$
$$\{a'_{i\varkappa}\} \equiv \{\beta_{i\varkappa}\} \equiv \{n_{i\varkappa}\} \pmod{p^t}$$
$$\cdots\cdots\cdots\cdots\cdots$$

und folglich

(54) $$\{a'_{i\varkappa}\} \equiv \{n_{i\varkappa}\} \pmod{N}.$$

Mit anderen Worten: Es giebt eine mit $f = \{a_{i\varkappa}\}$ äquivalente Form $f' = \{a'_{i\varkappa}\}$, welche der Congruenz (54) und somit sämmtlichen Congruenzen

(55) $$\{a'_{i\varkappa}\} \equiv \{\lambda_{i\varkappa}\} \pmod{2^{t_0}},\ \{a'_{i\varkappa}\} \equiv \{\mu_{i\varkappa}\} \pmod{p^t}, \cdots$$

Genüge leistet. Jede solche Form aus der Classe von

$$f = \{a_{i\varkappa}\}$$

wollen wir hinfort einen Hauptrepräsentanten dieser Classe (mod. N) nennen; die Formen zur Rechten der Congruenzen (55) sollen entsprechend Hauptreste von f nach den zugehörigen Moduln genannt werden. Bestehen die Congruenzen (55) nach den angedeuteten hinreichend hohen Potenzen als Moduln, so gelten sie auch nach den kleineren Potenzen; es genügt für unsere Zwecke, hinfort die Exponenten

$$t_0 > 1 + v_{n-1}(2),\ t > v_{n-1}(p)$$

u. s. w., das heisst N durch $2 o_1\, o_2 \cdots o_{n-1}$ theilbar anzunehmen, eine Annahme, die gewiss erfüllt ist, so oft wir N durch $2A$ theilbar voraussetzen, unter A die Determinante von f verstanden.

8. Hier müssen wir zunächst einen Hilfssatz entwickeln, der sogleich und auch später Verwendung finden wird. Sei q eine Primzahl und $|a_{i\varkappa}|$ eine Determinante mit n^2 beliebigen ganzzahligen Elementen; wir behalten für die Zeichen d_m, ∂_m, σ_m, v_m ihre frühere Bedeutung bei, setzen auch $t \gtreqless v_{n-1}$ voraus. Betrachten wir dann die Determinante $|a'_{i\varkappa}|$, deren Elemente denjenigen der ersteren Determinante (mod. q^t) congruent sind:

$$a'_{i\varkappa} = a_{i\varkappa} + \alpha_{i\varkappa} \cdot q^t.$$

Wird diese Determinante

$$|\, a_{i\varkappa} + \alpha_{i\varkappa} \cdot q^t \,|$$

nach den Potenzen von q^t entwickelt, so entsteht offenbar ein Ausdruck von folgender Gestalt:

$$(56)\quad \left\{ \begin{array}{l} |a_{i\varkappa}| + q^t \cdot \left(\begin{vmatrix} \alpha_{11} & a_{12} & \cdots \\ \alpha_{21} & a_{22} & \cdots \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & a_{n2} & \cdots \end{vmatrix} + \cdots \right) \\ + q^{2t} \cdot \left(\begin{vmatrix} \alpha_{11} & \alpha_{12} & a_{13} & \cdots \\ \alpha_{21} & \alpha_{22} & a_{23} & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{n1} & \alpha_{n2} & a_{n3} & \cdots \end{vmatrix} + \cdots \right) + \text{etc.} \end{array} \right.$$

Die Determinanten aber, welche in q^t multiplicirt sind, lassen sich als homogene lineare Funktionen von Unterdeterminanten $n-1^{\text{ten}}$ Grades von $|a_{i\varkappa}|$ darstellen, sind mithin sämmtlich theilbar durch $q^{\partial_{n-2}}$, die Glieder also, welche q^t enthalten, durch $q^{t+\partial_{n-2}}$. Gleicherweise werden die Glieder, welche q^{2t} enthalten, durch $q^{2t+\partial_{n-3}}$ theilbar sein und folglich, weil

$$t \geqq v_{n-1} \geqq v_{n-2} \text{ d. i. } \geqq \partial_{n-2} - \partial_{n-3}$$

also

$$2t + \partial_{n-3} \geqq t + \partial_{n-2}$$

ist, auch durch $q^{t+\partial_{n-2}}$, u. s. w. Man erhält also die Congruenz:

$$(57)\qquad |a'_{i\varkappa}| \equiv |a_{i\varkappa}| \pmod{q^{t+\partial_{n-2}}},$$

wenn $t \geqq v_{n-1}$ ist.

Dieses Resultat gilt für die Primzahl $q = 2$ so gut, wie für ungerade Primzahlen q. Nehmen wir aber an, die beiden Determinanten seien symmetrisch, d. h.

$$a_{\varkappa i} = a_{i\varkappa},\ \alpha_{\varkappa i} = \alpha_{i\varkappa},$$

so können wir das Resultat, welches dem Falle $q = 2$ entspricht, noch genauer formuliren. In dem Ausdrucke (56) werden dann die Glieder, welche 2^{2t} enthalten, wenn $t > v_{n-1}$ ist, durch $2 \cdot 2^{t+\partial_{n-2}}$ also jedenfalls auch durch $\sigma_{n-1} \cdot 2^{t+\partial_{n-2}}$ theilbar sein, und dasselbe gilt von den Gliedern mit den höheren Potenzen von 2^t. In den Gliedern aber, welche 2^t enthalten, werden diejenigen Theile der entwickelten Determinanten, welche in unsymmetrische Unterdetermi-

nanten von $|a_{i\varkappa}|$ multiplicirt sind, wie leicht zu übersehen, jetzt doppelt auftreten und somit alle Theile der entwickelten Determinanten durch $\sigma_{n-1}\cdot 2^{\partial_n-2}$, also die Glieder, welche 2^t enthalten, durch $\sigma_{n-1}\cdot 2^{t+\partial_n-2}$ theilbar sein. Die Congruenz (57) nimmt demnach unter der gegenwärtigen Annahme die neue Gestalt an:

$$(57a) \qquad |a'_{i\varkappa}| \equiv |a_{i\varkappa}| \pmod{\sigma_{n-1}\cdot 2^{t+\partial_n-2}}.$$

9. Wir setzen jetzt die Form $f=\theta^{(1)}$ als primitiv voraus. Wenn diese Form durch die Substitution (26) des vorigen Capitels in f' übergeht, so verwandelt sich nach dem in nr. 7 desselben gegebenen Satze auch $f^{(m)}$ durch die Substitution (71) daselbst in $f'^{(m)}$ und man erhält die nachstehenden Gleichungen:

$$(58) \quad \begin{cases} A'^{(1)}_{1,1} = a'_{11} = \theta^{(1)}(q_{\varrho 1}) \\ \frac{1}{d_1}\cdot A'^{(2)}_{12,12} = \theta^{(2)}(Q^{(2)}_{\varrho\sigma,12}) \\ \frac{1}{d_2}\cdot A'^{(3)}_{123,123} = \theta^{(3)}(Q^{(3)}_{\varrho\sigma\tau,123}) \\ \cdots\cdots\cdots\cdots \\ \frac{1}{d_{n-2}}\cdot A'^{(n-1)}_{12\cdots n-1,12\cdots n-1} = \theta^{(n-1)}(Q^{(n-1)}_{\varrho\sigma\tau\cdots,12\cdots n-1}); \end{cases}$$

zugleich ist einleuchtend, dass die Zahlen

$$Q^{(m)}_{\varrho\sigma\tau\cdots,12\cdots m}$$

welche in $\theta^{(m)}$ als Werthe der Unbestimmten auftreten, keinen gemeinsamen Theiler haben können, da die Determinante

$$|Q^{(m)}_{\varrho\sigma\tau\cdots,rst\cdots}|,$$

welche eine lineare homogene Funktion derselben ist, zugleich mit der Determinante $|q_{i\varkappa}|$ den Werth 1 hat (siehe Cap. 1, Formel (14a)). Wir werden demnach sagen, dass die Zahlen zur Linken der Gleichungen (58) gleichzeitig eigentlich durch die Formen $\theta^{(1)}, \theta^{(2)}, \cdots \theta^{(n-1)}$ dargestellt werden. Zur Abkürzung setzen wir allgemein

$$(59) \qquad \frac{1}{d_{m-1}}\cdot A'^{(m)}_{12\cdots m,12\cdots m} = \sigma_m\cdot f'_m$$

und fügen den so definirten $n-1$ ganzen Zahlen $f'_1, f'_2, \cdots f'_{n-1}$

noch die beiden hinzu:

(59) $$f_0' = 1,\ f_n' = (-1)^\tau.$$

In jedem Hauptrepräsentanten f' von f (mod. N) sind die Zahlen f_m' prim gegen N, wenn wir N theilbar durch $2A$ voraussetzen.

Denn, ist zuerst p^t eine der ungeraden Primzahlpotenzen von N, so genügt f' der Congruenz (25), aus welcher sich, da $t > v_{n-1} \geqq v_{m-1}$ gedacht wird, mittels des vorher entwickelten Hilfssatzes die folgende:

$$A'^{(m)}_{12\cdots m,\,12\cdots m} \equiv p^{\partial_{m-1}} \cdot \alpha\,\alpha' \cdots \alpha^{(m-1)} \pmod{p^{t+\partial_{m-2}}}$$

ergiebt. Setzt man

$$d_{m-1} = p^{\partial_{m-1}} \cdot \delta_m,$$

so folgt weiter

$$\delta_m \cdot \sigma_m f_m' \equiv \alpha\,\alpha' \cdots \alpha^{(m-1)} \pmod{p^{t - v_{m-1}}}$$

also auch (mod. p), woraus man erkennt, dass f_m' prim ist gegen p. — Das gleiche gilt für die anderen ungeraden Primfaktoren von N.

Aus der Congruenz (47) aber folgt nach dem Hilfssatze, wenn

$$m = \vartheta_{i-1} + h \quad (0 \leqq h < \varkappa_i)$$

gedacht wird, mit Rücksicht darauf, dass sich aus den Gleichungen (41) und (42)

$$\varkappa_2 \cdot v_{\vartheta_1} + \varkappa_3 \cdot v_{\vartheta_2} + \cdots + \varkappa_{i-1} \cdot v_{\vartheta_{i-2}} + h v_{\vartheta_{i-1}} = \partial_{m-1}$$

ergiebt,

$$A'^{(m)}_{12\cdots m,\,12\cdots m} \equiv \sigma_m \cdot 2^{\partial_{m-1}} \cdot U \pmod{\sigma_{m-1}\, 2^{t_0+\partial_{m-2}}},$$

wo U eine ungerade Zahl ist; und hieraus weiter, wenn jetzt $d_{m-1} = 2^{\partial_{m-1}} \cdot \delta_m$ gesetzt wird,

$$\delta_m \cdot \sigma_m f_m' \equiv \sigma_m \cdot U \pmod{\sigma_{m-1}\, 2^{t_0 - v_{m-1}}};$$

man findet demnach, da

$$t_0 > 1 + v_{n-1} \geqq 1 + v_{m-1}$$

gedacht wird,

$$\delta_m \cdot f_m' \equiv U \pmod{2}$$

d. i. f_m' ungerade. — Hiernach ist f_m' in der That prim gegen N.

Man kann aber den Hauptrepräsentanten

$$f' \pmod{N}$$

auch so wählen, dass in der Reihe der Zahlen f'_m je zwei benachbarte relativ prim sind. Gesetzt nämlich, bei f' sei dies noch nicht der Fall, z. B. sei f'_{m+1} nicht prim gegen f'_m, so setze man

$$f' = F' + G',$$

wo F' denjenigen Theil von f' bezeichnet, welcher nur die ersten $m+1$ Veränderlichen enthält. Wenn man dann auf f' eine Substitution $(t_{i\varkappa})$ mit dem Modulus 1 anwendet, welche nur diese Veränderlichen in ebenso viel andere verwandelt, so geht f' in eine äquivalente Form

$$f'' = F'' + G''$$

über, unter F'' die Transformirte von F' verstanden, sodass die Determinanten von F' und F'' übereinstimmen. Da nun offenbar $\sigma_{m+1} d_m \cdot f'_{m+1}$ gleich der Determinante von F',

$$\sigma_{m+1} d_m \cdot f''_{m+1}$$

gleich derjenigen von F'' ist, findet sich zunächst

$$f''_{m+1} = f'_{m+1}$$

und aus gleicher Ueberlegung finden sich auch

$$f''_{m+2} = f'_{m+2}, \; f''_{m+3} = f'_{m+3}, \cdots$$

Unter der Substitution $(t_{i\varkappa})$ darf aber eine solche verstanden werden, durch welche die Form F' in einen ihrer Hauptrepräsentanten mod. $(\sigma_{m+1} N f'_{m+1})$ übergeht; folglich dürfen

$$f''_1, f''_2, \cdots f''_m$$

prim gegen $\sigma_{m+1} N f'_{m+1}$, insbesondere also f''_m prim gegen

$$f'_{m+1} = f''_{m+1}$$

vorausgesetzt werden. Im allgemeinen braucht freilich die Form f'' dann kein Hauptrepräsentant von f (mod. N) mehr zu sein. Indessen lässt sich, da N und f'_{m+1} relativ prim sind, ähnlich wie in nr. 7 eine, nur die ersten $m+1$ Veränderlichen verwandelnde Substitution $(u_{i\varkappa})$ mit dem Modulus 1 so wählen, dass gleichzeitig

$$(u_{i\varkappa}) \equiv (t_{i\varkappa}) \text{ (mod. } f'_{m+1})$$

und

$$(u_{i\varkappa}) \equiv \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ . & . & . & . \\ 0 & 0 & \cdots & 1 \end{pmatrix} \text{ (mod. } N)$$

wird; entsteht durch diese Substitution aus $f' = F' + G'$ die Form

$$\varphi = \psi + \chi,$$

so leuchtet ein, dass einerseits wieder

$$\varphi_{m+1} = f'_{m+1} = f''_{m+1},$$

sowie

$$\varphi_{m+2} = f'_{m+2}, \quad \varphi_{m+3} = f'_{m+3} \cdots$$

sein werden; andererseits folgt

$$\varphi \equiv f' \text{ (mod. } N)$$

d. h. φ ist ein Hauptrepräsentant von f (mod. N) und daher φ_m prim gegen N; ebenso aber

$$\varphi \equiv f'' \text{ (mod. } f'_{m+1})$$

und folglich auch

$$\varphi_m \equiv f''_m \text{ (mod. } f'_{m+1}).$$

Da nun f''_m prim ist gegen

$$f''_{m+1} = f'_{m+1} = \varphi_{m+1},$$

so folgt endlich auch φ_m prim gegen φ_{m+1}.

Auf solche Weise verwandelt man den Hauptrepräsentanten f' (mod. N) in einen andern, in welchem die Zahlen f'_m, f'_{m+1} durch entsprechende relativ prime ersetzt sind, ohne dass die Zahlen mit einem grösseren Index als m dabei eine Aenderung erleiden. Und indem man in solcher Weise, von der letzten der Grössen f'_m ausgehend, den Repräsentanten, wenn nöthig, durch einen geeigneten anderen ersetzt, gelangt man schliesslich zu folgendem Satze:

Wird N theilbar durch $2A$ gedacht, so giebt es in der Classe von f einen Hauptrepräsentanten f' (mod. N), für welchen jede der Zahlen

(60) $$f'_0, f'_1, f'_2 \cdots f'_{n-1}, f'_n$$

nicht nur zu N, sondern auch zu den ihr benachbarten Zahlen prim ist.

Einen solchen Hauptrepräsentanten bezeichnet Smith*) als eine kanonische, Minkowski als eine charakteristische Form der Classe von f; wir ziehen letztere Bezeichnung vor, weil solche Form dazu dienen wird, die Geschlechtscharaktere der Classe zu bestimmen, und wir nennen aus gleichem Grunde die Zahlen (60) ein für die Form f oder f' charakteristisches System von Zahlen, ein Ausdruck, dessen wiederum schon Smith sich bedient hat.

10. Wir wenden uns nun dazu, die Geschlechtscharaktere einer Form zu ermitteln. Man kann sich zu diesem Zwecke, wie wir in der Theorie der ternären Formen gethan haben, der Grundformel bedienen, nach welcher

$$f(x_\varrho)\cdot f(y_\varrho)-[x_1 f^1(y_\varrho)+x_2 f^2(y_\varrho)+\cdots+x_n f^n(y_\varrho)]^2 \\ = f^{(2)}(x_\varrho y_\sigma - x_\sigma y_\varrho)$$

ist. Bildet man diese Gleichung nämlich für irgend eine der primitiven Begleitformen von f, z. B. für $\theta^{(m)}$, und nennt $\theta^{(m,2)}$ die zweite Begleitform der letzteren, so wird

$$(61)\quad \theta^{(m)}(x_\varrho)\cdot\theta^{(m)}(y_\varrho)-[x_1\theta^{(m)1}(y_\varrho)+\cdots+x_n\theta^{(m)n}(y_\varrho)]^2 \\ = \theta^{(m,2)}(x_\varrho y_\sigma - x_\sigma y_\varrho).$$

Der grösste gemeinsame Theiler aller Coefficienten von $\theta^{(m,2)}$ ist aber die Invariante o_m**). Andererseits können durch $\theta^{(m)}$ Zahlen oder doch das Doppelte solcher Zahlen dargestellt werden, welche prim sind gegen o_m. Bezeichnet man daher mit p_m irgend einen ungeraden Primfaktor von o_m und wählt die x_ϱ und y_ϱ auf alle Weisen so, dass $\theta^{(m)}(x_\varrho)$, $\theta^{(m)}(y_\varrho)$ prim wird gegen p_m, so lehrt die Gleichung (61) sogleich, dass alle diese Werthe von $\theta^{(m)}$ (mod. p_m) gleichen quadratischen Charakter, das Zeichen $\left(\frac{\theta^{(m)}}{p_m}\right)$ also einen bestimmten, unveränderlichen Werth hat. Mithin kommt der Form $\theta^{(m)}$ und damit

*) Smith, sur la représentation des nombres par une somme de cinq carrés, in Mém. prés. p. div. Sav. Etrangers etc. t. 29.

**) S. Smith a. a. O. Die Richtigkeit der Behauptung lässt sich mittels der unten benutzten Congruenzbetrachtungen bestätigen.

auch der Form f ein bestimmter, durch diesen Werth bezeichneter quadratischer Charakter (mod. p_m) zu.

Indem man diese Charaktere für die sämmtlichen primitiven Begleitformen $\theta^{(1)}, \theta^{(2)}, \cdots \theta^{(n-1)}$ der Form f mit Bezug auf die sämmtlichen ungeraden Primfaktoren der bezüglichen Invarianten $o_1, o_2, \cdots o_{n-1}$ aufstellt, erhält man das System der Hauptcharaktere (Smith) der Form f. Zu ihnen treten aber, analog wie bei den binären und ternären Formen, im allgemeinen noch andere hinzu, welche sich auf den Divisor 2 oder Potenzen desselben beziehen. Diese letzteren würden sich nur schwer aus der allgemeinen Grundformel entwickeln lassen und wir greifen daher auf die im Vorhergehenden abgeleiteten Congruenzbeziehungen, insbesondere auf die charakteristische Form zurück.

Wir benutzen zuerst die Formel (25), um das soeben aus der Grundformel Gewonnene wieder zu finden. — Wird unter p_m eine beliebige der Primzahlen verstanden, welche in o_m aufgehen, so ist die zugehörige Zahl ω_m von Null verschieden und wir erhalten, wenn f' irgend eine charakteristische Form der Classe von f (mod. N) und N eine durch $2A$ theilbare Zahl bezeichnet,

$$f' \equiv \begin{Bmatrix} \alpha & 0 & \cdots & 0 & 0 & \cdots \\ 0 & p_m^{\omega_1} \cdot \alpha' & \cdots & 0 & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & p_m^{\omega_1+\omega_2+\cdots+\omega_{m-1}} & \cdot\, \alpha^{(m-1)} & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots \end{Bmatrix} \pmod{p_m^{v_m}},$$

während $v_m > v_{m-1}$ ist. Die Unterdeterminante m^{ten} Grades von f', welche die ersten m Zeilen und Spalten enthält, wird hiernach und in Folge des Hilfssatzes mit Bezug auf den Modulus $p_m^{v_m+\partial_{m-2}}$ congruent sein mit

$$p_m^{\partial_{m-1}} \cdot \alpha\, \alpha' \cdots \alpha^{(m-1)},$$

woraus, wenn man $d_{m-1} = p_m^{\partial_{m-1}} \cdot \delta_m$ setzt, die Congruenz

$$(62) \qquad \delta_m \cdot \sigma_m f_m' \equiv \alpha\, \alpha' \cdots \alpha^{(m-1)} \pmod{p_m^{\omega_m}}$$

hervorgeht. Jede andere Unterdeterminante m^{ten} Grades enthält aber mindestens eine Reihe mit grösserem Index als m,

ist also die Summe der Produkte aus den durch $p_m^{\nu_m}$ theilbaren Gliedern dieser Reihe in Unterdeterminanten $m-1^{\text{ten}}$ Grades, mithin theilbar durch $p_m^{\nu_m+\partial_m-2}$. Sonach findet sich für alle ganzzahligen Werthe der Unbestimmten

$$f'^{(m)} \equiv p_m^{\partial_m-1} \cdot \alpha\,\alpha' \cdots \alpha^{(m-1)} \cdot x^2 \pmod{p_m^{\nu_m+\partial_m-2}}$$

und daraus

$$\theta'^{(m)} \equiv \sigma_m f'_m \cdot x^2 \pmod{p_m^{\omega_m}}.$$

Also erhält $\theta'^{(m)}$ nur dann einen durch p_m nicht theilbaren Werth, wenn man x durch p_m nicht theilbar wählt, und für alle so entstehenden Werthe von $\theta'^{(m)}$ findet sich

$$\left(\frac{\theta'^{(m)}}{p_m}\right) = \left(\frac{\sigma_m f'_m}{p_m}\right).$$

Aber die Formen $\theta^{(m)}$ und $\theta'^{(m)}$ sind einander äquivalent und stellen daher auch dieselben Zahlen dar; daher überträgt sich der constante Werth von $\left(\frac{\theta'^{(m)}}{p_m}\right)$ sogleich auf das Symbol $\left(\frac{\theta^{(m)}}{p_m}\right)$. Der voraufgehenden Gleichung zufolge ist er mit dem Werthe, welchen das Symbol $\left(\frac{f'_m}{p_m}\right)$ für irgend eine charakteristische Form der Classe von f besitzt, zugleich bestimmt. Wir nennen deshalb den Werth dieses Symbols

$$\left(\frac{f'_m}{p_m}\right) \tag{63}$$

einen Charakter der Form f, allgemeiner ihrer Classe.

11. Um auch die supplementären Charaktere der Form f, d. i. diejenigen Charaktere festzustellen, die sich auf den Divisor 2 resp. seine Potenzen beziehen, müssen wir anknüpfen an die Congruenz (47), nach welcher

$$f' \equiv \varphi \pmod{2^{\nu\vartheta_i}} \tag{64}$$

gesetzt werden darf, wo

$$\varphi = \sum_{\varkappa=1}^{i-1} 2^{\nu\vartheta_\varkappa-1} \cdot \Phi_\varkappa + 2^{\nu\vartheta_i-1} \cdot \sum_{s=1}^{\varkappa_i} \alpha_s^{(i)} \xi_s^{(i)2} \tag{64a}$$

oder

$$(64\text{b})\begin{cases} \varphi = \sum_{\varkappa=1}^{i-1} 2^{v_{\vartheta_\varkappa -1}} \cdot \Phi_\varkappa \\ + 2^{v_{\vartheta_i -1}} \cdot \sum_{s=1}^{\frac{1}{2}\varkappa_i} (2\alpha_s^{(i)} \xi_s^{(i)2} + 2\mathfrak{A}_s^{(i)} \xi_s^{(i)} \xi_s'^{(i)} + 2\mathfrak{a}_s^{(i)} \xi_s'^{(i)2}), \end{cases}$$

jenachdem die Form Φ_i erster oder zweiter Art ist. Nun kann jede Zahl m der Reihe $1, 2, 3, \cdots n-1$ nur entweder einer der Zahlen $\vartheta_1, \vartheta_2, \cdots \vartheta_{\lambda-1}$ gleich oder zwischen zwei aufeinanderfolgenden der Zahlen $\vartheta_0, \vartheta_1, \vartheta_2, \cdots \vartheta_\lambda$ enthalten sein; setzen wir demnach

$$m = \vartheta_{i-1} + h,$$

indem wir unter h eine der Zahlen $0, 1, 2 \cdots \varkappa_i - 1$ verstehen, und untersuchen die Unterdeterminanten m^{ten} Grades von f'. Enthielte eine solche mindestens eine Reihe, deren Index $> \vartheta_i$ ist, so wäre sie als Summe der Produkte der Glieder dieser Reihe in Unterdeterminanten $m-1^{\text{ten}}$ Grades nach (47) theilbar durch

$$2^{v_{\vartheta_i}} \cdot \sigma_{m-1}\, 2^{\partial_m - 2}.$$

Jede Unterdeterminante m^{ten} Grades von f' aber, welche nur Reihen enthält, deren Indices $\overline{\gtrless}\, \vartheta_i$ sind, ist dem Hilfssatze (nr. 8) zufolge der entsprechenden Unterdeterminante von φ

$$(\text{mod. } 2^{v_{\vartheta_i}} \cdot \sigma_{m-1}\, 2^{\partial_m - 2})$$

congruent. Hiernach findet sich für die m^{ten} Begleitformen von f' und φ folgende Congruenz:

$$(65) \qquad f'^{(m)} \equiv \varphi^{(m)} \; (\text{mod. } \sigma_{m-1} \cdot 2^{v_{\vartheta_i} + \partial_m - 2}).$$

Da aber $v_{\vartheta_i} > v_m$ also $2^{v_{\vartheta_i}}$ durch $\sigma_{m+1} \cdot 2^{v_m}$ und daher

$$\sigma_{m-1} \cdot 2^{v_{\vartheta_i} + \partial_m - 2} \text{ durch } \sigma_{m-1} \cdot 2^{\omega_m} \cdot \sigma_{m+1} \cdot 2^{\partial_m - 1}$$

theilbar ist, müssen die Coefficienten von $\varphi^{(m)}$, wie es diejenigen von $f'^{(m)}$ sind, sämmtlich durch $2^{\partial_m - 1}$ theilbar sein und die Congruenz nimmt, wenn man wieder

$$d_{m-1} = 2^{\partial_m - 1} \cdot \delta_m$$

setzt, folgende Gestalt an:

$$(66) \qquad \delta_m \cdot \theta'^{(m)} \equiv \frac{\varphi^{(m)}}{2^{\partial_m - 1}} \pmod{2^{\mu_m}}.$$

Ist insbesondere $m = \vartheta_{i-1}$ also $\sigma_m = 1$, so ist diejenige Unterdeterminante m^{ten} Grades von φ, welche aus den ersten m Zeilen und Spalten besteht, gleich

$$\prod_{x=1}^{i-1} (\Phi_x) \cdot 2^{\partial_m - 1},$$

wenn man unter (Φ_x) die Determinante der Form Φ_x versteht, sie ist also, getheilt durch $2^{\partial_m - 1}$, eine gewisse ungerade Zahl. Jede andere Unterdeterminante m^{ten} Grades von φ enthält mindestens eine Reihe, deren Glieder durch $2^{^v\vartheta_i - 1}$ theilbar sind, und ist deshalb theilbar durch

$$2^{^v\vartheta_i - 1} \cdot \sigma_{m-1} 2^{\partial_m - 2},$$

ja sogar durch

$$2^{^v\vartheta_i - 1} \cdot \sigma_{m-1} 2^{\partial_m - 2} \sigma_{m+1} = 2^{\mu_m} \cdot 2^{\partial_m - 1},$$

wenn für φ die Formel (64a) gilt, also $\sigma_{m+1} = 1$ ist. Im entgegengesetzten Falle wird für die symmetrischen Unterdeterminanten dasselbe gelten, da sie theilbar sind durch

$$2 \cdot 2^{^v\vartheta_i - 1} \sigma_{m-1} 2^{\partial_m - 2};$$

weil aber die unsymmetrischen in $\varphi^{(m)}$ doppelt genommen vorkommen, findet sich offenbar aus (66),

wenn $m = \vartheta_{i-1}$ ist, für alle ganzzahligen Werthe der Unbestimmten die besondere Congruenz:

$$(67) \qquad \delta_m \cdot \theta'^{(m)} \equiv \prod_{x=1}^{i-1} (\Phi_x) \cdot x^2 \pmod{2^{\mu_m}}.$$

Demzufolge kann die Form $\theta'^{(m)}$ nur dann ungerade Werthe erhalten, wenn man x ungerade wählt, und man ersieht sofort, dass alle ungeraden Werthe dieser Form

wenn $\mu_m \geqq 2$ ist, der Congruenz

$$\delta_m \cdot \theta'^{(m)} \equiv \prod_{x=1}^{i-1} (\Phi_x) \pmod{4},$$

wenn $\mu_m > 3$ ist, der Congruenz

$$\vartheta_m \cdot \theta'^{(m)} \equiv \prod_{x=1}^{i-1} (\Phi_x) \pmod{8}$$

Genüge leisten.

Ist also $m = \vartheta_{i-1}$ und $\mu_m \gtreqless 2$, so kommt der Form $\theta'^{(m)}$ und somit auch der äquivalenten Form $\theta^{(m)}$ ein bestimmter Charakter (mod. 4) zu, insofern der Ausdruck $(-1)^{\frac{\theta^{(m)}-1}{2}}$ für alle ungeraden durch $\theta^{(m)}$ darstellbaren Zahlen den gleichen Werth hat. — Ist $\mu \gtreqless 3$, so gilt ausserdem dasselbe (mod. 8), insofern auch der Werth des Symbols $\left(\frac{2}{\theta^{(m)}}\right)$ für alle ungeraden durch $\theta^{(m)}$ darstellbaren Zahlen unveränderlich ist. Diesen Werth eines jeden der angegebenen Ausdrücke bezeichnen wir wieder als einen Charakter der Form f.

Offenbar ist

$$\delta_m \cdot f'_m \equiv \prod_{x=1}^{i-1} (\Phi_x) \pmod{2^{\mu_m}},$$

und demnach kann man den supplementären Charakter, welchen die Form f in den angegebenen Fällen nach den Moduln 4 oder 8 besitzt, durch den Werth kennzeichnen, welchen das Symbol

$$(-1)^{\frac{1}{2}(f'_m-1)} \text{ resp. } (-1)^{\frac{1}{8}(f'^2_m-1)} = \left(\frac{2}{f'_m}\right)$$

für irgend eine charakteristische Form f' der Classe von f besitzt.

12. Wenn $\mu_m < 2$ ist, kommt im allgemeinen der Form $\theta'^{(m)}$ oder $\theta^{(m)}$ kein quadratischer Charakter der durch sie dargestellten Zahlen mit Bezug auf 4 oder 8 zu. Untersuchen wir aber noch die in nr. 6 hervorgehobenen zwei letzten Annahmen.

Sei also zuerst

$$\mu_m = 1,\ \mu_{m-1} \gtreqless 2,\ \mu_{m+1} \gtreqless 2.$$

Diese Annahme bedingt, dass gleichzeitig

$$m - 1 = \vartheta_{i-2},\ m = \vartheta_{i-1},\ \omega_m = 1,\ m + 1 = \vartheta_i$$

und φ von folgender Form ist:

$$\varphi = \sum_{x=1}^{i-2} 2^{v\vartheta_x - 1}\Phi_x + 2^{v\vartheta_i - 2}\cdot\alpha\xi^2 + 2^{v\vartheta_i - 2}\cdot 2\alpha'\xi'^2.$$

Da hiernach, wenn $\omega_{m+1} > 1$ ist — was nach 5) nr. 6 jedenfalls zutrifft, sobald Φ_{i+1} erster Art ist —

$$v_{\vartheta_i} = v_{\vartheta_{i-1}} + \omega_{\vartheta_i} \overline{\overline{>}}\, v_m + 2,$$

folglich wegen $\sigma_{m+1} = 1$

$$\sigma_{m-1}\cdot 2^{v\vartheta_i + \partial_m - 2} \text{ durch } 4\cdot\sigma_{m-1}\, 2^{\omega_m}\,\sigma_{m+1}\cdot 2^{\partial_m - 1}$$

theilbar ist, erschliesst man aus der Congruenz (65) hier die folgende:

$$(68)\qquad \delta_m\cdot\theta'^{(m)} \equiv \frac{\varphi^{(m)}}{2^{\partial_m - 1}} \pmod{4\cdot 2^{\mu_m}} \text{ d. i. } \pmod{8}.$$

Ist aber Φ_{i+1} zweiter Art und zugleich $\omega_{m+1} = 1$, so wird, wenn

$$\psi = \varphi + 2^{v\vartheta_i}\cdot\Phi_{i+1}$$

gesetzt wird, wegen $v_{\vartheta_{i+1}} > v_{\vartheta_i}$ analog mit (68) diese Congruenz:

$$\delta_m\cdot\theta'^{(m)} \equiv \frac{\psi^{(m)}}{2^{\partial_m - 1}} \pmod{8}$$

hervorgehen, und ähnlich wie bei (67) überzeugt man sich, dass dann wenigstens für alle ganzzahligen Werthe der Unbestimmten die Congruenz (68) erfüllt ist. Mit Rücksicht darauf, dass, wenn Φ_{i-2} erster Art ist, $\omega_{m-1} > 1$ sein muss, folgt daraus ebenfalls für alle ganzzahligen Werthe der Unbestimmten die Congruenz:

$$(69)\quad \delta_m\cdot\theta'^{(m)} \equiv \prod_{x=1}^{i-2}(\Phi_x)\cdot\alpha x^2 + \prod_{x=1}^{i-2}(\Phi_x)\cdot 2\alpha' x'^2 \pmod{8}.$$

Daher erhält $\theta'^{(m)}$ nur dann ungerade Werthe, wenn x ungerade gewählt wird, während x' beliebig gerade oder ungerade gewählt werden darf. Hieraus ergiebt sich leicht, dass der Ausdruck zur Rechten, so oft die Zahlen

$$(70)\qquad \prod_{x=1}^{i-2}(\Phi_x)\cdot\alpha \text{ und } \prod_{x=1}^{i-2}(\Phi_x)\cdot\alpha'$$

congruent sind oder, was dasselbe sagt, so oft ihr Produkt

congruent 1 ist (mod. 4), entweder nur Zahlen von den Formen $8n+1, 3$ oder nur Zahlen von den Formen $8n+5, 7$ annehmen kann, im entgegengesetzten Falle entweder nur Zahlen von den Formen $8n+3, 5$ oder nur solche von den Formen $8n+1, 7$; mit anderen Worten: im ersteren Falle hat das Symbol

$$(-1)^{\frac{1}{2}(\delta_m \theta'^{(m)}-1)} \cdot \left(\frac{2}{\delta_m \theta'^{(m)}}\right)$$

und folglich auch dieses:

$$(-1)^{\frac{1}{2}(\theta'^{(m)}-1)} \cdot \left(\frac{2}{\theta'^{(m)}}\right),$$

im zweiten Falle das Symbol $\left(\frac{2}{\delta_m \theta'^{(m)}}\right)$ und folglich auch das andere:

$$\left(\frac{2}{\theta'^{(m)}}\right)$$

einen unveränderlichen Werth.

Nun kommt aber dem Vorigen zufolge den Formen

$$\theta'^{(m-1)} \text{ und } \theta'^{(m+1)}$$

ein Charakter (mod. 4) zu, dem entsprechend die beiden Congruenzen

$$\delta_{m-1} \cdot f'_{m-1} \equiv \prod_{\varkappa=1}^{i-2} (\Phi_\varkappa), \quad \delta_{m+1} \cdot f'_{m+1} \equiv \prod_{\varkappa=1}^{i-2} (\Phi_\varkappa) \cdot \alpha\alpha' \pmod{4}$$

bestehen, und den letzteren gemäss ist das Produkt der beiden Zahlen (70) congruent mit

$$\delta_{m-1}\,\delta_{m+1} \cdot f'_{m-1} f'_{m+1}$$

oder, da man leicht

$$\delta_{m-1}\,\delta_{m+1} = e_m \cdot \delta_m^2 \tag{71}$$

findet, wenn

$$o_m = 2^{\omega_m} \cdot e_m \tag{72}$$

gesetzt wird, congruent mit

$$e_m \;\; f'_{m-1} f'_{m+1} \pmod{4}.$$

Indem man noch der Form $\theta'^{(m)}$ die äquivalente Form $\theta^{(m)}$ substituirt, gelangt man schliesslich zu folgendem Resultate:

Unter der gemachten Annahme kommt der Form $\theta^{(m)}$ ein bestimmter quadratischer Charakter zu, indem,

wenn

$$e_m f'_{m-1} \cdot f'_{m+1} \equiv 3 \pmod{4}$$

ist, das Symbol $\left(\frac{2}{\theta^{(m)}}\right)$,

wenn

$$e_m f'_{m-1} \cdot f'_{m+1} \equiv 1 \pmod{4}$$

ist, das Symbol $(-1)^{\frac{1}{2}(\theta^{(m)}-1)} \cdot \left(\frac{2}{\theta^{(m)}}\right)$

für alle ungeraden Werthe von $\theta^{(m)}$ den gleichen Werth hat. Man darf, da $\sigma_m = 1$ ist, diese Charaktere durch die Werthe kennzeichnen, welche das erste resp. zweite der Symbole

$$\left(\frac{2}{f'_m}\right), \quad (-1)^{\frac{1}{2}(f'_m-1)} \cdot \left(\frac{2}{f'_m}\right)$$

für irgend eine charakteristische Form f' der Classe von f besitzt.

Sei zweitens $\mu_m = 0$, zugleich aber

$$\mu_{m-1} \overline{\overline{>}} 2, \; \mu_{m+1} \overline{\overline{>}} 2 \text{ und } \sigma_m = 1;$$

dann muss nach 6) nr. 6 $m = \vartheta_{i-1} + 1$ sein und φ folgende Gestalt haben:

$$\varphi = \sum_{\varkappa=1}^{i-1} 2^{\nu\vartheta_{\varkappa-1}} \cdot \Phi_\varkappa + 2^{\nu\vartheta_{i-1}} \cdot (\alpha\xi^2 + \alpha'\xi'^2),$$

woraus $\sigma_{m+1} = 1$ hervorgeht. Der Modulus der Congruenz (65) lässt sich also schreiben:

$$\sigma_{m-1} 2^{\omega_m} \sigma_{m+1} \cdot 2^{\omega_{m+1}+\partial_{m-1}} = 2^{\omega_{m+1}+\partial_{m-1}},$$

und folglich ergiebt sich aus derselben, so oft $\omega_{m+1} > 1$ ist, was jedenfalls zutrifft, sobald Φ_{i+1} erster Art ist, die folgende:

$$(73) \qquad \delta_m \cdot \theta'^{(m)} \equiv \frac{\varphi^{(m)}}{2^{\partial_{m-1}}} \pmod{4}$$

oder nach der Gestalt von φ:

$$(74) \qquad \delta_m \cdot \theta'^{(m)} \equiv \prod_{\varkappa=1}^{i-1} (\Phi_\varkappa) \cdot \alpha x^2 + \prod_{\varkappa=1}^{i-1} (\Phi_\varkappa) \cdot \alpha' x'^2 \pmod{4}.$$

Ist Φ_{i+1} zweiter Art und zugleich $\omega_{m+1} = 1$, so findet sich zunächst, wie im vorigen Falle, wenn man

$$\psi = \varphi + 2^{\nu \vartheta_i} \Phi_{i+1}$$

setzt, jedenfalls die Congruenz

$$\delta_m \cdot \theta'^{(m)} \equiv \frac{\psi^{(m)}}{2^{\partial_m - 1}} \pmod{4}.$$

Da nun aber jede Unterdeterminante m^{ten} Grades von ψ, welche wenigstens eine zu Φ_{i+1} gehörige Reihe enthält, wenn sie symmetrisch ist, und jede unsymmetrische doppelt genommen, wie sie in der vorigen Congruenz vorkommt, auch nach Division mit $2^{\partial_m - 1}$ noch durch 4 theilbar sein muss, wird

$$\frac{\psi^{(m)}}{2^{\partial_m - 1}} \equiv \frac{\varphi^{(m)}}{2^{\partial_m - 1}} \pmod{4}$$

und somit die Congruenz (74) wenigstens für alle ganzzahligen Werthe der Unbestimmten wieder erfüllt. Ihr zufolge wird aber $\theta'^{(m)}$ einen quadratischen Charakter (mod. 4) haben oder nicht haben, jenachdem das Produkt der beiden Zahlen

$$\prod_{x=1}^{i-1} (\Phi_x) \cdot \alpha, \quad \prod_{x=1}^{i-1} (\Phi_x) \cdot \alpha' \tag{75}$$

congruent 1 oder 3 ist (mod. 4), und man erschliesst also, ganz wie im vorigen Falle, den Satz: Jenachdem

$$e_m f'_{m-1} f'_{m+1} \equiv 1 \text{ oder } 3 \text{ ist } \pmod{4},$$

kommt der Form $\theta^{(m)}$ ein quadratischer Charakter (mod. 4) zu oder nicht; im ersteren Falle hat also das Symbol $(-1)^{\frac{\theta^{(m)}-1}{2}}$ einen für alle ungeraden Werthe von $\theta^{(m)}$ unveränderlichen Werth, der mit dem Werthe des Symbols $(-1)^{\frac{f'_m - 1}{2}}$ zugleich bestimmt ist.

13. Noch erübrigt, den Fall zu untersuchen, in welchem m eine der Zahlen *zwischen* ϑ_{i-1} und ϑ_i und $\mu_m = 2$ ist. Φ_i ist dann von der zweiten Art und wir erhalten die Congruenz

$$f' \equiv \varphi \pmod{2^{\nu \vartheta_i}},$$

wo

$$\varphi = \sum_{\varkappa=1}^{i-1} 2^{{}^v\vartheta_\varkappa - 1} \cdot \Phi_\varkappa$$

$$+ 2^{{}^v\vartheta_i - 1} \cdot \sum_{s=1}^{\frac{1}{2}\varkappa_i} (2\alpha_s \xi_s^2 + 2\mathfrak{A}_s \xi_s \xi_s' + 2\mathfrak{a}_s \xi_s'^2)$$

ist; zur grösseren Anschaulichkeit schreiben wir

$$\varphi = \left|\begin{array}{cccccc} \square & & & & & \\ \cdot\ \cdot & 2^{{}^v\vartheta_i-1}\cdot 2\alpha_1, & 2^{{}^v\vartheta_i-1}\cdot\mathfrak{A}_1 & & & \\ \cdot\ \cdot & 2^{{}^v\vartheta_i-1}\cdot\mathfrak{A}_1, & 2^{{}^v\vartheta_i-1}\cdot 2\mathfrak{a}_1 & & & \\ \cdot\ \cdot\ \cdot & & \cdot & 2^{{}^v\vartheta_i-1}\cdot 2\alpha_2, & 2^{{}^v\vartheta_i-1}\cdot\mathfrak{A}_2 & \cdots \\ \cdot & \cdot & \cdot & 2^{{}^v\vartheta_i-1}\cdot\mathfrak{A}_2, & 2^{{}^v\vartheta_i-1}\cdot 2\mathfrak{a}_2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right.$$

indem wir durch das kleine Quadrat diejenigen Glieder umfassen, welche den Formen $\Phi_1, \Phi_2, \cdots \Phi_{i-1}$ angehören. Wir wollen hier zwei Zeilen oder zwei Spalten, welche durch dasselbe der viergliedrigen Quadrate hindurchgehen, ein Paar zusammengehöriger Zeilen resp. Spalten nennen. Nun ist

$$m = \vartheta_{i-1} + 2h < \vartheta_i$$

und folglich gilt die Congruenz (66) d. i. die folgende

$$(76) \qquad \delta_m \cdot \theta'^{(m)} \equiv \frac{\varphi^{(m)}}{2^{\partial_m - 1}} \pmod{4}.$$

Eine Unterdeterminante m^{ten} Grades von φ enthält aber mindestens $2h$ Zeilen oder Spalten, welche Φ_i angehören. Enthält sie, was sicher der Fall ist, wenn sie unsymmetrisch in Bezug auf die ersten ϑ_{i-1} Reihen gebildet ist, mehr als $2h$ solcher Zeilen oder Spalten, so ist sie nach Division mit $2^{\partial_m - 1}$ mindestens noch durch

$$2^{{}^v\vartheta_{i-1} - {}^v\vartheta_{i-2}} = 2^{{}^\omega\vartheta_{i-1}}$$

also durch 2 theilbar; ist sie unsymmetrisch, so kommt sie zur Rechten von (76) doppelt genommen vor, kann also, wo es sich nur um ganze Werthe der Unbestimmten handelt, unterdrückt werden; ist sie symmetrisch, enthält aber nicht

lauter Paare zusammengehöriger Reihen, so wird sie nach Division mit $2^{\partial_m - 1}$ sogar noch durch $2 \cdot 2^{\omega\vartheta_i - 1}$ also durch 4 theilbar sein und unterdrückt werden können; enthält sie aber lauter Paare zusammengehöriger Reihen, so enthält sie mindestens $2h + 2$ Reihen aus Φ_i und kann weggelassen werden, da sie nach Division mit $2^{\partial_m - 1}$ noch durch $2^{\nu\vartheta_{i-1} + \omega\vartheta_{i-1}}$ also durch 4 aufgeht. Enthält dagegen die Unterdeterminante nur $2h$ Reihen aus Φ_i, darunter jedoch nur $2h'$, welche Paare zusammengehöriger Reihen sind, so enthält sie mindestens zwei nicht zusammengehörige Reihen und wird, wenn sie symmetrisch ist, nach Division mit $2^{\partial_m - 1}$ noch durch 4 theilbar also wegzulassen sein. Man denke sich also auf alle

$$c = \frac{\frac{1}{2}\varkappa_i\left(\frac{1}{2}\varkappa_i - 1\right)\cdots\left(\frac{1}{2}\varkappa_i - h + 1\right)}{1\cdot 2\cdots h}$$

mögliche Arten h Paare zusammengehöriger Reihen aus Φ_i ausgewählt und beachte, dass

$$2\alpha_s \cdot 2\mathfrak{a}_s - \mathfrak{A}_s^2 \equiv -1 \pmod{4}$$

ist, so wird aus (76) für alle ganzzahligen Werthe der Unbestimmten folgende Congruenz hervorgehen:

$$(77)\quad \delta_m \cdot \theta'^{(m)} \equiv (-1)^h \cdot \prod_{\varkappa=1}^{i-1}(\Phi_\varkappa)\cdot(x_1^2 + x_2^2 + \cdots + x_c^2) + \cdots \pmod{4},$$

in welcher wir durch die Punkte zur Rechten eine Reihe doppelter Produkte zweier Unbestimmten mit *ungeraden* Coefficienten andeuten.

Z. B. fände man für $\varkappa_i = 4$ und $h = 1$:

$$\delta_m \cdot \theta'^{(m)} \equiv -\prod_{\varkappa=1}^{i-1}(\Phi_\varkappa)\cdot[x_{12}^2 + x_{34}^2 + 2\mathfrak{A}_1\mathfrak{A}_2(x_{13}x_{24} + x_{14}x_{23})] \pmod{4}.$$

Hieraus geht aber hervor, dass im gegenwärtigen Falle der Form $\theta'^{(m)}$ *kein* quadratischer Charakter (mod. 4) zukommt*); denn, damit z. B. in dem besonderen

*) Dies ist Smith's Darstellung der Sache entgegen zu halten (s. art. 6 seiner Arbeit).

letzten Falle $\theta'^{(m)}$ ungerade wird, muss eine der Zahlen x_{12}, x_{34} gerade, die andere ungerade sein, und dann lässt $\delta_m \cdot \theta'^{(m)}$, jenachdem man $x_{13}x_{24} + x_{14}x_{23}$ gerade oder ungerade wählt, einen oder den andern der Reste ± 1 (mod. 4); also gestattet $\theta'^{(m)}$ Zahlen beider Restformen $4n \pm 1$ die Darstellung.

Aber es zeigt sich hier ein anderer Gesichtspunkt, von dem aus man der Form $\theta'^{(m)}$ auch in diesem Falle einen quadratischen Charakter beilegen kann. Bezeichnet man nämlich mit $\sigma_m d_{m-1}(f'_m)$ oder vielmehr, da hier $\sigma_m = 1$ ist, mit $d_{m-1}(f'_m)$ jede der symmetrischen oder Hauptunterdeterminanten m^{ten} Grades von f', so zeigt die Congruenz (77), dass für alle diejenigen von ihnen, bei welchen (f'_m) ungerade ist, (f'_m) den gleichen quadratischen Charakter (mod. 4) hat, der durch denjenigen des Produktes $\prod_{x=1}^{i-1} (\Phi_x)$ bestimmt wird. Da f'_m zu $2A$ prim also eine dieser Zahlen ist, so kann der Werth, welchen das Symbol $(-1)^{\frac{1}{2}(f'_m - 1)}$ hat, den gedachten quadratischen Charakter kennzeichnen. Es ist einleuchtend, dass auch in den früheren Fällen dieser neue Gesichtspunkt zur Bestimmung des quadratischen Charakters der Form f' angewandt werden kann und mit dem erstgewählten sich vollkommen deckt, da die bezeichneten Zahlen (f'_m) sämmtlich Werthe sind, welche durch die Form $\theta'^{(m)}$ eigentlich dargestellt werden können. Von diesem andern Gesichtspunkte aus hat im Unterschiede von Smith, dem wir bisher gefolgt sind, Minkowski die Geschlechtseintheilung der Formen entwickelt. Da er, wie man aus dem letzten Falle ersieht, erschöpfender ist als der erste, werden wir hinfort gleichfalls von demselben ausgehen. Aber, während in den übrigen Fällen die Charakterisirung — auf die eine wie die andere Art — völlig unabhängig war von der beliebigen Wahl der charakteristischen Form f', die man der Betrachtung zu Grunde legt, bleibt dies offenbar im letzten Falle noch erst zu erweisen.

Denkt man sich also statt f' irgend eine andere charakteristische Form ausgewählt, so wird nachzuweisen sein, dass

das Produkt $\prod_{\varkappa=1}^{i-1}(\Phi_\varkappa)$, welches in (77) auftritt, dadurch (mod. 4) keine Aenderung erleidet. Hierzu bemerke man vor allem, dass durch die veränderte Wahl von f' die mit φ bezeichnete Form nur insofern eine Aenderung erleidet, als die Coefficienten der einzelnen Formen $\Phi_\varkappa$ andere werden; bei der Bestimmung des Produktes $\prod_{\varkappa=1}^{i-1}(\Phi_\varkappa)$ (mod. 4) wird aber solche Aenderung bezüglich derjenigen Formen $\Phi_\varkappa$, welche zweiter Art sind, ohne Einfluss sein, da die Determinante einer solchen immer einen bestimmten der beiden Werthe $+1$ oder -1 (mod. 4) hat. Es wird also genügen, ein Produkt $\prod_{\varkappa=1}^{h-1}(\Phi_\varkappa)$ unter der Voraussetzung zu betrachten, dass Φ_{h-1} eine Form der ersten, Φ_h eine Form der zweiten Art ist. Dann ist aber für $m = \vartheta_{h-1}$ (nach nr. 6) $\mu_m \gtreqless 2$; nach nr. 11 kommt daher der Form $\theta'^{(m)}$ ein besonderer Charakter (mod. 4) zu, und da der Werth $\delta_m \theta'^{(m)}$ für jede Wahl der charakteristischen Form dem entsprechenden Produkte

$$\prod_{\varkappa=1}^{h-1}(\Phi_\varkappa) \quad (\text{mod. } 4)$$

congruent ist, hat auch das letztere einen, von jener Wahl unabhängigen quadratischen Charakter (mod. 4)*).

14. Lässt man nun m die Werthe

$$\vartheta_{i-1},\ \vartheta_{i-1}+2,\ \vartheta_{i-1}+4,\ \cdots \vartheta_i$$

durchlaufen, so wird den entsprechenden Formen $\theta'^{(m)}$ dem Bewiesenen zufolge ein Charakter

$$(-1)^{\frac{1}{2}(f'_m-1)}$$

zukommen, zu dessen Bestimmung die Congruenzen

*) Bezüglich der Supplementarcharaktere ist zu beachten, dass, wie unsere Herleitung zeigt, die zu ihrer Bestimmung dienende Form f' nicht durchaus eine charakteristische Form der Classe, sondern allgemeiner nur ein Hauptrepräsentant derselben zu sein braucht.

$$\left.\begin{aligned}
&\text{für } m = \vartheta_{i-1}: \\
&\qquad \delta_m f'_m \equiv \prod_{\varkappa=1}^{i-1} (\Phi_\varkappa) \\
&\text{für } m = \vartheta_{i-1} + 2h: \\
&\qquad \delta_m f'_m \equiv (-1)^h \cdot \prod_{\varkappa=1}^{i-1} (\Phi_\varkappa) \\
&\text{für } m = \vartheta_i: \\
&\qquad \delta_m f'_m \equiv \prod_{\varkappa=1}^{i} (\Phi_\varkappa) \equiv (-1)^{\frac{1}{2}\varkappa_i} \cdot \prod_{\varkappa=1}^{i-1} (\Phi_\varkappa)
\end{aligned}\right\} \pmod{4}$$

dienen. Ihnen entsprechend findet sich für die genannten Werthe von $m < \vartheta_i - 2$ die Beziehung

$$\delta_m f'_m \equiv -\delta_{m+2} \cdot f'_{m+2} \pmod{4},$$

der man nach (71) die Form

$$f'_m \cdot f'_{m+2} \equiv -e_{m+1} \pmod{4} \tag{78}$$

geben kann, sodass die Gleichung

$$(-1)^{\frac{1}{2}(f'_m - 1)} \cdot (-1)^{\frac{1}{2}(f'_{m+2} - 1)} = (-1)^{\frac{1}{2}(e_{m+1} + 1)} \tag{79}$$

hervorgeht. Man sieht also, dass die Charaktere, welche der bezeichneten Reihe von Formen zukommen, nicht unabhängig von einander sind; insbesondere findet sich, wenn man das vorige Produkt für alle angegebenen Werthe von m bildet, welche $< \vartheta_i$ sind, und die so entstehenden Formeln multiplicirt, zwischen den Charakteren, welche

$$m = \vartheta_{i-1} \text{ und } m = \vartheta_i$$

zugehören, nachstehende Beziehung:

$$\left\{\begin{aligned}
&(-1)^{\frac{1}{2}(f'_{\vartheta_{i-1}} - 1)} \cdot (-1)^{\frac{1}{2}(f'_{\vartheta_i} - 1)} \\
&= (-1)^{\frac{1}{2}\varkappa_i} \cdot (-1)^{\frac{1}{2}(e_{\vartheta_{i-1}+1} \cdot e_{\vartheta_{i-1}+3} \cdots e_{\vartheta_i - 1} - 1)}.
\end{aligned}\right. \tag{80}$$

Ueberhaupt aber ist zu bemerken, dass die von uns festgestellten einzelnen Charaktere einer Form f nicht ganz unabhängig von einander sind, sodass sie nicht nach Belieben gewählt werden dürfen, sondern gewissen Bedingungen genügen müssen, wenn eine Form f der gegebenen Ordnung mit den gewählten

Charakteren vorhanden sein soll. Man gelangt zu diesen Bedingungen folgendermassen:

Sei nach wie vor f' eine charakteristische Form der Classe von f, so folgt aus der, das Zeichen f'_m definirenden Gleichung

$$\sigma_m \cdot f'_m = \frac{1}{d_{m-1}} \cdot A'^{(m)}_{12\cdots m;\,12\cdots m} \tag{81}$$

und aus der bekannten Determinantenbeziehung

$$\left\{\begin{aligned} & A'^{(m)}_{12\cdots m;\,12\cdots m} \cdot A'^{(m-2)}_{12\cdots m-2;\,12\cdots m-2} \\ = & A'^{(m-1)}_{12\cdots m-2,m-1;\,12\cdots m-2,m-1} \cdot A'^{(m-1)}_{12\cdots m-2,m;\,12\cdots m-2,m} \\ & - (A'^{(m-1}_{12\cdots m-2,m;\,12\cdots m-2,m-1})^2 \end{aligned}\right. \tag{82}$$

die Gleichung

$$o_{m-1} \cdot \sigma_m f'_m \cdot \sigma_{m-2} f'_{m-2} = \sigma^2_{m-1} \cdot f'_{m-1} \cdot {}'f_{m-1} - F^2, \tag{83}$$

wenn man die letztgeschriebenen beiden Unterdeterminanten, durch $\sigma_{m-1} d_{m-2}$ resp. durch d_{m-2} getheilt, mit $'f_{m-1}$ und F resp. bezeichnet, oder die nachstehende Congruenz

$$- \sigma_{m-2}\, o_{m-1}\, \sigma_m \cdot f'_{m-2} f'_m \equiv F^2 \pmod{\sigma^2_{m-1} \cdot f'_{m-1}}. \tag{84}$$

Diese Congruenzbeziehung, welche die Zahlen f'_m unter sich verknüpft, bedingt damit zugleich die Abhängigkeit der Einzelcharaktere von einander.

Setzt man $m+2$ statt m und beachtet, dass $\sigma_m\, o_{m+1}\, \sigma_{m+2}$ ungerade, mithin $o_{m+1} = e_{m+1}$ ist, so oft $\sigma_{m+1} = 2$ ist (s. nr. 6), so fliesst aus der allgemeinen Congruenz (84) unter dieser besonderen Voraussetzung stets diese andere:

$$f'_m \cdot f'_{m+2} \equiv - e_{m+1} \pmod{4}. \tag{84a}$$

Da für die zuvor betrachteten Werthe

$$m = \vartheta_{i-1},\ \vartheta_{i-1} + 2,\ \vartheta_{i-1} + 4,\ \cdots \vartheta_i - 2$$

die Voraussetzung $\sigma_{m+1} = 2$ zutreffend ist, findet sich so die Congruenz (78) sammt ihren Folgerungen von Neuem bewiesen und als besonderer Fall unter der allgemeinen Bedingung (84) enthalten.

Wir verstehen unter ε_m (für $m = 0, 1, 2, \cdots n$) diejenige positive oder negative Einheit, welche dasselbe Zeichen hat wie f'_m, sodass $\varepsilon_m f'_m$ positiv ist, und folgern weiter aus (84),

indem wir m in $m+1$ verwandeln, die Gleichung:

$$(85)\qquad \left(\frac{-2^{\mu_m} e_m}{f'_m}\right)\cdot\left(\frac{f'_{m-1}}{f'_m}\right)\cdot\left(\frac{f'_{m+1}}{f'_m}\right)=1.$$

Wir stellen dieselbe für jeden der Werthe

$$m=1,2,\cdots n-1$$

auf und multipliciren die so entstehenden Gleichungen in einander. Bedenkt man dabei, dass

$$\left(\frac{2^{\mu_m}}{f'_m}\right)=(-1)^{\mu_m\cdot\frac{1}{8}(f'^2_m-1)}$$

ist, berücksichtigt die Werthe

$$f'_0=1,\ f'_n=(-1)^\tau$$

und dass nach dem verallgemeinerten Reciprocitätsgesetze

$$\left(\frac{f'_{m-1}}{f'_m}\right)\cdot\left(\frac{f'_m}{f'_{m-1}}\right)=(-1)^{\frac{1}{4}(\varepsilon_{m-1}-1)(\varepsilon_m-1)+\frac{1}{4}(f'_{m-1}-1)(f'_m-1)}$$

und

$$\left(\frac{e_m}{f'_m}\right)=\left(\frac{f'_m}{e_m}\right)\cdot(-1)^{\frac{f'_m-1}{2}\cdot\frac{e_m-1}{2}}$$

ist, so gelangt man ohne Schwierigkeit zur folgenden Gleichung:

$$(86)\qquad (-1)^{\varepsilon(o,n-1)+\psi(o,n-1)}=\prod_{m=1}^{n-1}\left(\frac{f'_m}{e_m}\right),$$

in welcher zur Abkürzung

$$(87)\quad \varepsilon(o,n-1)=\sum_{m=1}^{n-1}\frac{\varepsilon_m-1}{2}+\sum_{m=1}^{n}\frac{1}{4}(\varepsilon_{m-1}-1)(\varepsilon_m-1)$$

und

$$(88)\quad \begin{cases} \psi(o,n-1) \\ =\sum_{m=1}^{n-1}\mu_m\cdot\frac{1}{8}(f'^2_m-1)+\sum_{m=1}^{n-1}\frac{(f'_m-1)(e_m+1)}{4} \\ \qquad +\sum_{m=1}^{n-1}\frac{(f'_m-1)(f'_{m+1}-1)}{4} \end{cases}$$

gesetzt ist. Man kann bemerken, dass in der Potenz

$$(-1)^{\psi(o,n-1)}$$

nur diejenigen f'_m verbleiben, für welche $\sigma_m = 1$ ist; denn die Theile des Ausdrucks $\psi(o, n-1)$, in denen f'_m vorkommt, sind

$$\mu_m \cdot \frac{1}{8}(f'^2_m - 1) + \frac{f'_m - 1}{2}\left(\frac{e_m + 1}{2} + \frac{f'_{m-1} - 1}{2} + \frac{f'_{m+1} - 1}{2}\right),$$

wo nun, so oft $\sigma_m = 2$ ist, der erste Summande wegen des Faktors $\mu_m = 0$, der zweite, weil er in Folge der Congruenz (84a) eine gerade Zahl ist, im Exponenten der Potenz

$$(-1)^{\psi(o, n-1)}$$

unterdrückt werden kann.

Die Einheit $(-1)^{s(o, n-1)}$ ist unabhängig von der Wahl der charakteristischen Form f'. Denn, da die Zahlen

$$f'_0, f'_1, f'_2, \cdots f'_{n-1}, f'_n$$

ungerade, also von Null verschieden sind, findet sich nach der Formel von Jacobi (vor. Cap. (119)) die Gleichung:

$$(89) \qquad f' = \frac{X_1^2}{f'_0 f'_1} + \frac{X_2^2}{f'_1 f'_2} + \cdots + \frac{X_n^2}{f'_{n-1} f'_n},$$

in welcher die X_i reelle lineare Funktionen der Unbestimmten von f' sind, und, wie man auch f' in der Classe von f gewählt habe, die Anzahl der negativen Summanden zur Rechten gleich τ ist. Mithin sind von den Produkten

$$\varepsilon_0 \varepsilon_1, \ \varepsilon_1 \varepsilon_2, \cdots \varepsilon_{n-1} \varepsilon_n$$

τ gleich -1, die übrigen gleich $+1$. Jenachdem nun $\varepsilon_{m-1}\varepsilon_m$ gleich $+1$ oder -1 ist, findet sich

$$\frac{1}{4}(\varepsilon_{m-1} + 1)(\varepsilon_m - 1) \equiv 0 \text{ oder } \equiv \frac{1}{2}(\varepsilon_m - 1) \pmod{2}$$

und daher ist

$$\sum_{m=1}^{n} \frac{1}{4}(\varepsilon_{m-1} + 1)(\varepsilon_m - 1) \equiv \sum \frac{1}{2}(\varepsilon_m - 1) \pmod{2},$$

wenn die Summe rechts auf alle m der zweiten Art bezogen wird; diese Summe giebt an, wie oft zur Rechten von (89) ein Wechsel vom Positiven zum Negativen stattfindet, ist also gleich $\frac{\tau}{2}$ oder $\frac{\tau+1}{2}$, jenachdem τ gerade oder ungerade ist.

Nun ist

$$\varepsilon(o, n-1) = \sum_{m=1}^{n} \frac{1}{4}(\varepsilon_{m-1}+1)(\varepsilon_m - 1) - \frac{\varepsilon_n - 1}{2}$$

und $\frac{\varepsilon_n - 1}{2} \equiv \tau \pmod{2}$, also findet man

$$\varepsilon(o, n-1) \equiv \tau + \frac{\tau}{2} \text{ resp. } \tau + \frac{\tau+1}{2}$$

d. h. allgemein

$$\varepsilon(o, n-1) \equiv \left[\frac{\tau}{2}\right] \pmod{2}$$

und

$$(-1)^{\varepsilon(o, n-1)} = (-1)^{\left[\frac{\tau}{2}\right]},$$

wenn $\left[\frac{\tau}{2}\right]$, wie üblich, das grösste in $\frac{\tau}{2}$ enthaltene Ganze bezeichnet.

Angenommen nun, für die Form f seien die sämmtlichen $\mu_m < 2$ d. h. die sämmtlichen σ-Invarianten gleich 1, die o-Invarianten ungerade oder das Doppelte ungerader Zahlen, so wird zwar der Form f dem Obigen gemäss kein einzelner Charakter nach einem der Moduln 4 oder 8 zukommen. Aber aus der Gleichung (86) geht hervor, dass $(-1)^{\psi(o, n-1)}$ in diesem Falle einen Werth hat, welcher von der Wahl der charakteristischen Form unabhängig ist, und aus diesem Grunde nennt Smith diese Einheit einen, in dem angegebenen Falle der Form f und ihren primitiven Begleitformen zukommenden *Simultancharakter*.

Die im Vorigen gewonnenen Ergebnisse genügen für die Folge und so übergehen wir hier weitere Folgerungen, welche aus der Congruenzbeziehung (84) für andere besondere Fälle fliessen (s. darüber die Arbeiten von Smith und Minkowski).

15. Fassen wir aber die Untersuchungen der letzten Nummern zusammen, so ergiebt sich folgendes: Jeder Form f kommt eine gewisse (endliche) Anzahl quadratischer Charaktere zu; bildet man nämlich eine charakteristische Form f' der Classe von f, so werden gewisse, aus den Werthen f'_m gebildete Einheiten einen unveränderlichen Werth haben, wie immer die Form f' auch gewählt wird. Diese Einheiten

heissen die Charaktere der Form f oder auch ihrer Classe. Sie sind

1) die Symbole $\left(\frac{f'_m}{p_m}\right)$, welche den verschiedenen in o_m aufgehenden ungeraden Primfaktoren entsprechen;

2) wenn $\mu_m \gtreqless 2$ ist, die Einheiten $(-1)^{\frac{1}{2}(f'_m-1)}$;

3) wenn $\mu_m \gtreqless 3$ ist, ausserdem die Einheiten

$$(-1)^{\frac{1}{8}(f'^2_m-1)};$$

4) wenn $\mu_{m-1} \gtreqless 2$, $\mu_m = 1$, $\mu_{m+1} \gtreqless 2$ ist, die Einheiten

$$(-1)^{\frac{1}{8}(f'^2_m-1)} \text{ resp. } (-1)^{\frac{1}{8}(f'^2_m-1)+\frac{1}{2}(f'_m-1)},$$

jenachdem $e_m f'_{m-1} f'_{m+1} \equiv \mp 1 \pmod{4}$ ist;

5) wenn $\mu_{m-1} \gtreqless 2$, $\mu_m = 0$, $\mu_{m+1} \gtreqless 2$, $\sigma_m = 1$ und

$$e_m f'_{m-1} f'_{m+1} \equiv +1 \pmod{4}$$

ist, die Einheit $(-1)^{\frac{1}{2}(f'_m-1)}$.

Zwischen diesen Charakteren besteht eine Abhängigkeit, die in der Congruenz

$$(90) \qquad -\sigma_{m-1}\, o_m\, \sigma_{m+1} \cdot f'_{m-1} f'_{m+1} \equiv F^2 \pmod{\sigma_m^2 \cdot f'_m}$$

begründet ist. Unter den dieselbe aussprechenden Bedingungen heben wir besonders die Gleichung (86) in der Gestalt:

$$(91) \qquad (-1)^{\left[\frac{\tau}{2}\right]} = (-1)^{\psi(o,n-1)} \cdot \prod_{m=1}^{n-1} \left(\frac{f'_m}{e_m}\right)$$

hier hervor, indem wir sie als **Bedingung** für die Möglichkeit der Charaktere bezeichnen.

Es ist einleuchtend, dass für alle Classen einer gegebenen Ordnung dieselben Categorieen und in jeder von ihnen dieselbe Reihe von Einzelcharakteren vorhanden sein werden, denn durch die Ordnung allein werden sowohl die Primzahlen p_m als auch die Werthe der Zahlen μ_m bestimmt. Denkt man sich nun für die gegebene Ordnung diese ihre Einzelcharaktere aufgestellt, so wollen wir alle diejenigen Classen, welchen gleiche Einzelcharaktere d. i. die gleichen *Werthe* der bezeichneten Einheiten zukommen, als ein *Geschlecht*

von Classen — und da die Charaktere der Classen sich sogleich auch auf die Formen übertragen und umgekehrt — als ein Geschlecht von Formen definiren. Auf solche Weise zerfallen demnach alle Formen einer Ordnung in eine Anzahl verschiedener Geschlechter. Die Anzahl der unterscheidbaren Geschlechter kann nur eine endliche sein, da die Anzahl der möglichen Einzelcharaktere also auch die Anzahl ihrer mit der Bedingung (90) oder (91) verträglichen Werthcombinationen nur eine endliche ist.

16. Sei $\mathfrak{f}$ die Reciproke von f mit umgekehrter Reihenfolge ihrer Veränderlichen und sei ebenso $\mathfrak{f}'$ die Reciproke von f' mit umgekehrter Reihenfolge ihrer Veränderlichen. Wir behaupten den Satz: Die charakteristische Form f' der Classe von f kann so gewählt werden, dass die Form $\mathfrak{f}'$ zugleich eine charakteristische Form der Classe von $\mathfrak{f}$ ist.

In der That, ist p zuerst eine der ungeraden Primzahlen, welche in dem Modulus N aufgehen, auf den sich die charakteristische Form bezieht und der immer durch $2A$ theilbar zu denken ist, so darf man f' der Congruenz

$$f' \equiv \begin{Bmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & p^{\omega_1}\alpha' & 0 & \cdots & 0 \\ 0 & 0 & p^{\omega_1+\omega_2}\alpha'' & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & p^{\omega_1+\omega_2+\cdots+\omega_{n-1}} \cdot \alpha^{(n-1)} \end{Bmatrix} \pmod{p^t}$$

$(t > \epsilon_{n-1})$ gemäss gewählt denken, aus welcher sich für die Reciproke $\mathfrak{f}'$ folgende andere ergiebt:

$$\mathfrak{f}' \equiv \begin{Bmatrix} \beta^{(n-1)} \cdot p^{\omega_1'+\omega_2'+\cdots+\omega_{n-1}'} & 0 & \cdots & & 0 \\ 0 & \beta^{(n-2)} \cdot p^{\omega_1'+\cdots+\omega_{n-2}'} & \cdots & & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \beta' \cdot p^{\omega_1'} & 0 \\ 0 & 0 & \cdots & 0 & \beta \end{Bmatrix} \pmod{p^{t-\epsilon_{n-2}}},$$

wenn die Zahlen $\beta, \beta', \cdots \beta^{(n-1)}$ mit den Zahlen $\alpha, \alpha', \cdots \alpha^{(n-1)}$ durch nachstehende Congruenzen:

$$\delta_{n-1} \cdot \beta^{(n-1)} \equiv (-1)^{\tau} \cdot \frac{\varpi}{\alpha},$$

$$\delta_{n-1} \cdot \beta^{(n-2)} \equiv (-1)^{\tau} \cdot \frac{\varpi}{\alpha'}, \cdots \delta_{n-1} \cdot \beta \equiv (-1)^{\tau} \cdot \frac{\varpi}{\alpha^{(n-1)}}$$

$$(\text{mod. } p^{t-v_{n-1}-v_{n-2}}),$$

in denen ϖ für $\alpha\alpha' \cdots \alpha^{(n-1)}$ steht, verbunden sind; δ_{n-1} ist in bekannter Weise durch die Gleichung

$$d_{n-2} = p^{\partial_{n-2}} \cdot \delta_{n-1}$$

bestimmt. Den letzteren Congruenzen zufolge sind

$$\beta, \beta', \cdots \beta^{(n-1)}$$

durch p nicht-theilbare Zahlen. Kehrt man demnach die Reihenfolge der Variabeln $x_1, x_2, \cdots x_n$ in $\mathfrak{f}'$ um, so wird, falls t gross genug gedacht wird, $\mathbf{f}'$ jedenfalls zu einem Hauptrepräsentanten der Classe von $\mathbf{f}$, mit welcher die Form $\mathbf{f}'$ ebenso äquivalent ist, wie $\mathfrak{f}'$ mit $\mathfrak{f}$, nach einer beliebig hohen Potenz $p^{t'}$ als Modulus.

Dasselbe erkennt man bei Benutzung der Congruenz (31) auf genau dieselbe Weise mit Bezug auf den Modulus 2^t, sobald die Determinante A ungerade vorausgesetzt wird und $\sigma_1 = 1$ ist. — Ist dagegen bei ungerader Determinante $\sigma_1 = 2$, so gilt für die Form f' die Congruenz (40); aus dieser aber lässt sich auf demselben Wege für $\mathfrak{f}'$ leicht nachstehende Congruenz herleiten:

$$\mathfrak{f}' \equiv \begin{Bmatrix} 2\mathfrak{b}, & \mathfrak{B}, & 0\ 0 \cdots 0 & 0 \\ \mathfrak{B}, & 2b, & 0\ 0 \cdots 0 & 0 \\ \cdot & \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 & 0\ 0 \cdots 2\mathfrak{b}^{\left(\frac{n}{2}-1\right)}, & \mathfrak{B}^{\left(\frac{n}{2}-1\right)} \\ 0 & 0 & 0\ 0 \cdots \mathfrak{B}^{\left(\frac{n}{2}-1\right)}, & 2b^{\left(\frac{n}{2}-1\right)} \end{Bmatrix} (\text{mod. } 2^{t'}),$$

in welcher $b, b', \cdots b^{\left(\frac{n}{2}-1\right)}$ ebenso wie $\mathfrak{B}, \mathfrak{B}', \cdots \mathfrak{B}^{\left(\frac{n}{2}-1\right)}$ ungerade Zahlen sind. Und so zeigt sich wieder, dass $\mathbf{f}'$ zu einem Hauptrepräsentanten (mod. 2^t) der Classe von $\mathbf{f}$ wird.

In dem Falle endlich, in welchem f' eine gerade Form

mit einer ungeraden Anzahl von Unbestimmten ist, deren sämmtliche o-Invarianten ungerade sind bis auf die letzte, die das Doppelte einer ungeraden Zahl sein soll, würde f' als Hauptrepräsentant (mod. 2^t) folgenden Rest geben:

$$f' \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0, & 0, & \cdots 0 & 0 & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0, & 0, & \cdots 0 & 0 & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & \cdots 2a^{(i)}, & \mathfrak{A}^{(i)}, & 0 \\ 0 & 0 & 0 & 0 & \cdots \mathfrak{A}^{(i)}, & 2\mathfrak{a}^{(i)}, & 0 \\ 0 & 0 & 0 & 0 & \cdots 0 & 0 & 2a^{(i+1)} \end{Bmatrix} \pmod{2^t},$$

in welchem $a, \mathfrak{A}, \cdots a^{(i)}, \mathfrak{A}^{(i)}, a^{(i+1)}$ ungerade Zahlen sind. Da

$$\omega_1 = \omega_2 = \cdots = \omega_{n-2} = 0$$

also

$$\partial_{n-2} = 0$$

ist, würde man hieraus für die Reciproke $\mathbf{f}'$ mit umgekehrter Reihenfolge ihrer Veränderlichen die Congruenz gewinnen:

$$\mathbf{f}' \equiv \begin{Bmatrix} b & 0 & 0 & \cdots 0 & \\ 0 & 4b_1 & 2\mathfrak{B}_1 & \cdots 0 & \\ 0 & 2\mathfrak{B}_1 & 4\mathfrak{b}_1 & \cdots 0 & \\ . & . & . & . & . \\ 0 & 0 & 0 & \cdots 4b_i & 2\mathfrak{B}_i \\ 0 & 0 & 0 & \cdots 2\mathfrak{B}_i & 4\mathfrak{b}_i \end{Bmatrix} \pmod{2^t},$$

wo $b, b_1, \mathfrak{B}_1, \cdots b_i, \mathfrak{B}_i$ ungerade Zahlen bedeuten, d. i.

$$\mathbf{f}' \equiv bx^2 + 2 \cdot \sum_{s=1}^{i} (2b_s y_s^2 + 2\mathfrak{B}_s y_s z_s + 2\mathfrak{b}_s z_s^2) \pmod{2^t},$$

was in der That die Form eines Hauptrepräsentanten (mod. 2^t) für die Ordnung ist, der $\mathbf{f}'$ angehört, da ihre o-Invarianten diejenigen von f' in umgekehrter Reihenfolge, nämlich

$$\omega_1' = 1, \; \omega_2' = \omega_3' = \cdots = \omega_{n-1}' = 0$$

sind.

Für unsere Zwecke wird es genügen, den behaupteten Satz für die erörterten Fälle zu beweisen, wir ziehen darum keine weiteren in Betracht.

oder vielmehr die Bestimmung der Anzahl ihrer Wurzeln oder incongruenten Lösungen. Die quadratische Form darf dabei durchweg als prim gegen N vorausgesetzt werden. Wir bezeichnen dann die gesuchte Anzahl durch das Zeichen $f\{\alpha, N\}$. Es wird uns genügen, diese Anzahl für den Fall zu ermitteln, wo N eine Primzahlpotenz q^t ist.

Uebrigens lässt sich der allgemeine Fall sehr einfach auf diesen besonderen zurückführen. Denn, ist die Zahl N aus den Primzahlen $q^t, q'^{t'}, \cdots$ zusammengesetzt, so leuchtet zuerst ein, dass jeder Wurzel x_ϱ der Congruenz (1) auch je eine Wurzel

$$(2) \qquad \xi_\varrho \equiv x_\varrho \pmod{q^t}, \quad \xi_\varrho' \equiv x_\varrho \pmod{q'^{t'}}, \cdots$$

der Congruenzen

$$(3) \qquad f(\xi_\varrho) \equiv \alpha \pmod{q^t}, \quad f(\xi_\varrho') \equiv \alpha \pmod{q'^{t'}}, \cdots$$

zugeordnet ist. Bestimmt man aber umgekehrt zu je einer Wurzel $\xi_\varrho, \xi_\varrho', \cdots$ dieser letzteren Congruenzen die Zahl x_ϱ gemäss den Congruenzen (2), was stets auf eindeutige Weise geschehen kann, so findet man

$$f(x_\varrho) \equiv \alpha \pmod{q^t}, \quad f(x_\varrho) \equiv \alpha \pmod{q'^{t'}}, \cdots$$

also auch

$$f(x_\varrho) \equiv \alpha \pmod{N}$$

und somit gehört zu jedem Systeme von Wurzeln der Congruenzen (3) eine Wurzel der Congruenz (1). Demgemäss ist die Anzahl der Wurzeln der letzteren gleich der Anzahl der Systeme von Wurzeln der einzelnen Congruenzen (3).

Indem wir nun zuvörderst α durch q nicht theilbar voraussetzen, führen wir den Fall, in welchem der Modulus eine Potenz von q ist, auf denjenigen zurück, wo q selbst der Modulus ist. Hierzu dienen die folgenden Betrachtungen*):

1) Sei q eine ungerade Primzahl p und α nicht theilbar durch p. Eine Wurzel

$$x_\varrho \equiv \xi_\varrho \pmod{p^t}$$

der Congruenz

$$(4) \qquad f(x_\varrho) \equiv \alpha \pmod{p^t},$$

*) S. Minkowski, Untersuchungen über quadratische Formen, Acta Mathem. Bd. 7 S. 213.

in welcher $t > 1$ gedacht werde, ist stets zugleich auch eine Wurzel der Congruenz

$$(5)\qquad f(x_\varrho) \equiv \alpha \pmod{p^{t-1}};$$

aber auch umgekehrt erhält man aus jeder Wurzel

$$\xi_\varrho \pmod{p^{t-1}}$$

der letzteren nicht nur eine, sondern p^{n-1} verschiedene Wurzeln der ersteren. In der That, setzt man

$$(6)\qquad x_\varrho = \xi_\varrho + p^{t-1} \cdot z_\varrho, \quad (\varrho = 1, 2, \cdots n)$$

so wird

$$f(x_\varrho) = f(\xi_\varrho) + p^{t-1} \cdot \sum_{i=1}^{n} z_i \cdot \frac{\partial f(\xi_\varrho)}{\partial \xi_i} + p^{2t-2} \cdot f(z_\varrho)$$

d. i., da

$$f(\xi_\varrho) = \alpha + p^{t-1} \cdot \xi$$

gesetzt werden darf,

$$f(x_\varrho) - \alpha \equiv p^{t-1} \cdot \left(\xi + \sum_i z_i \frac{\partial f(\xi_\varrho)}{\partial \xi_i}\right) \pmod{p^t}.$$

Nun muss eine der Zahlen

$$\frac{\partial f(\xi_\varrho)}{\partial \xi_i} \quad (\text{für } i = 1, 2, \cdots n)$$

prim gegen p sein, da

$$\sum_i \xi_i \cdot \frac{\partial f(\xi_\varrho)}{\partial \xi_i} = 2 \cdot f(\xi_\varrho) \equiv 2\alpha \pmod{p^{t-1}}$$

also nicht durch p theilbar ist; somit kann man, wie aus nr. 4 des vierten Capitels leicht hervorgeht, die Werthe

$$z_1, z_2, \cdots z_n \pmod{p}$$

auf p^{n-1} verschiedene Weisen so wählen, dass

$$\xi + \sum_i z_i \frac{\partial f(\xi_\varrho)}{\partial \xi_i} \equiv 0 \pmod{p}$$

mithin

$$f(x_\varrho) \equiv \alpha \pmod{p^t}$$

wird. Auf solche Weise erhält man mittels der Formeln (6) aus je einer Wurzel von (5) je p^{n-1} (mod. p^t) verschiedene Wurzeln der Congruenz (4). Daher wird die Anzahl der Wurzeln der letzteren p^{n-1} Mal so gross sein als die Anzahl

der Wurzeln der ersteren. Hieraus aber folgt offenbar der Satz:

Ist A die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{p},$$

so ist $A \cdot p^{(n-1)(t-1)}$ die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{p^t}.$$

2) Sei nun $f(x_\varrho)$ eine ungerade Form und α eine ungerade Zahl. Man bemerke dann zunächst, dass, wenn

$$x_\varrho \equiv \xi_\varrho \pmod{2^t}$$

eine Wurzel der Congruenz

$$(7) \qquad f(x_\varrho) \equiv \alpha \pmod{2^t},$$

in welcher $t > 3$ gedacht werde, bedeutet, dann stets ein System von 2^n nach dem Modulus 2^{t-1} congruenten Wurzeln vorhanden ist, welche durch die Formel

$$x_\varrho = \xi_\varrho + 2^{t-1} \cdot z_\varrho$$
$$(\varrho = 1, 2, 3, \cdots n)$$

dargestellt werden, wenn man darin die z_ϱ gleich 0 oder 1 wählt; denn für jeden dieser Werthe der z_ϱ findet sich

$$f(x_\varrho) \equiv f(\xi_\varrho) + 2^t \cdot \sum_i z_i \cdot \frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i} \equiv f(\xi_\varrho) \pmod{2^t}.$$

Andererseits folgt aus der Wurzel $x_\varrho \equiv \xi_\varrho$ der Congruenz (7) zugleich auch

$$f(\xi_\varrho) \equiv \alpha \pmod{2^{t-1}}$$

und somit aus jedem Systeme von 2^n nach dem Modulus 2^{t-1} congruenten Wurzeln von (7) eine Wurzel also auch ein System von 2^n nach dem Modulus 2^{t-2} congruenten Wurzeln der Congruenz

$$(8) \qquad f(x_\varrho) \equiv \alpha \pmod{2^{t-1}}.$$

Ist aber umgekehrt $x_\varrho \equiv \xi_\varrho \pmod{2^{t-1}}$ eine beliebige aus einem solchen Systeme von Wurzeln der letzteren Congruenz und wählt man

$$(9) \qquad x_\varrho = \xi_\varrho + 2^{t-2} \cdot z_\varrho,$$
$$(\varrho = 1, 2, 3, \cdots n)$$

so folgt

$$f(x_\varrho) = f(\xi_\varrho) + 2^{t-1} \cdot \sum_i z_i \cdot \frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i} + 2^{2t-2} \cdot f(z_\varrho)$$

d. i., da man

$$f(\xi_\varrho) = \alpha + 2^{t-1} \cdot \xi$$

setzen darf,

$$f(x_\varrho) - \alpha \equiv 2^{t-1}\left(\xi + \sum_i z_i \cdot \frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i}\right) \pmod{2^t}.$$

Nun muss wegen der Congruenz (8), deren linke Seite gleich

$$\sum_i \xi_i \cdot \frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i}$$

ist, wenigstens eine der Zahlen

$$\frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i} \quad (\text{für } i = 1, 2, \cdots n)$$

ungerade sein; nach nr. 4 des vierten Capitels hat daher die Congruenz

$$\xi + \sum_i z_i \cdot \frac{1}{2} \frac{\partial f(\xi_\varrho)}{\partial \xi_i} \equiv 0 \pmod{2}$$

2^{n-1} Wurzeln, die man erhält, indem man $n - 1$ der Zahlen z_ϱ beliebig, eine von ihnen aber passend (mod. 2) wählt. Es ist mithin möglich

$$f(x_\varrho) \equiv \alpha \pmod{2^t}$$

zu machen, aus der Wurzel ξ_ϱ von (8) also eine solche x_ϱ von (7) herzuleiten. Da man hierbei $n - 1$ der Zahlen z_ϱ jeden Werth, einer von ihnen aber nur einen Werth (mod. 2) beilegen, der Formel (9) also die Gestalt

$$x_\varrho = (\xi_\varrho + 2^{t-2} z_\varrho') + 2^{t-1} \cdot \zeta_\varrho$$
$$(\varrho = 1, 2, \cdots n)$$

geben darf, in welcher ζ_ϱ sowie $n - 1$ der Zahlen z_ϱ' jeden Werth, ein z_ϱ' jedoch nur einen Werth (mod. 2) erhalten können, so repräsentirt diese Formel 2^{n-1} Systeme von je 2^n nach dem Modulus 2^{t-1} congruenten Wurzeln der Congruenz (7). So ergiebt sich: Die Anzahl der Systeme von je 2^n (mod. 2^{t-1}) congruenten Wurzeln der Congruenz (7) ist 2^{n-1} mal grösser als die Anzahl der Systeme von je 2^n (mod. 2^{t-2}) congruenten Wurzeln der Congruenz (8), und so-

mit ist auch die Anzahl aller Wurzeln jener Congruenz 2^{n-1} mal grösser als die Anzahl aller Wurzeln der letzteren. Hieraus schliesst man aber offenbar wieder den Satz:

Ist A die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{8},$$

so ist $A \cdot 2^{(n-1)(l-3)}$ die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{2^l}.$$

Handelt es sich nicht um sämmtliche Wurzeln der Congruenzen, sondern nur um diejenigen, welche (mod. 2) vorgeschriebene Reste haben, so wird sich an den Schlussfolgerungen, wie ohne Mühe zu übersehen ist, nichts wesentliches ändern und somit der erhaltene Satz auch dann in Giltigkeit sein.

3) Ist endlich $f(x_\varrho)$ eine gerade Form, während α ungerade ist, so kann die Congruenz (7) nicht stattfinden, wohl aber die Congruenz

$$f(x_\varrho) \equiv 2\alpha \pmod{2^l}, \tag{10}$$

welche, wenn man

$$\varphi(x_\varrho) = \frac{1}{2} f(x_\varrho)$$

setzt, mit der anderen

$$\varphi(x_\varrho) \equiv \alpha \pmod{2^{l-1}} \tag{11}$$

völlig gleichbedeutend ist; nur leuchtet ein, dass immer je 2^n Wurzeln der ersteren zu einer Wurzel der letzteren gehören, indem aus jeder Wurzel der ersteren eine solche der letzteren, umgekehrt aber aus jeder Wurzel dieser stets 2^n Wurzeln der ersteren hervorgehen. Dies wird, wie leicht ersichtlich, auch dann der Fall bleiben, wenn wir die Betrachtung nur auf solche Lösungen x_ϱ beschränken, bei denen nicht sämmtliche Ausdrücke

$$\frac{1}{2}\frac{\partial f(x_\varrho)}{\partial x_i} \quad (\text{für } i = 1, 2, \cdots n) \tag{12}$$

gerade sind. Nun folgt aus jeder Wurzel

$$x_\varrho \equiv \xi_\varrho \pmod{2^{l-1}}$$

von (11) auch eine Wurzel $x_\varrho \equiv \xi_\varrho \pmod{2^{l-2}}$ der Congruenz

(13) $$\varphi(x_\varrho) \equiv \alpha \pmod{2^{t-2}};$$

umgekehrt: bedeutet ξ_ϱ eine Wurzel dieser letzteren und wählt man

(14) $$x_\varrho = \xi_\varrho + 2^{t-2} \cdot z_\varrho, \quad (\varrho = 1, 2, \cdots n)$$

so folgt, $t > 2$ gedacht,

$$\varphi(x_\varrho) \equiv \varphi(\xi_\varrho) + 2^{t-2} \cdot \sum_i z_i \cdot \frac{\partial \varphi(\xi_\varrho)}{\partial \xi_i} \pmod{2^{t-1}}$$

oder, da man

$$\varphi(\xi_\varrho) = \alpha + 2^{t-2} \cdot \xi$$

setzen darf,

$$\varphi(x_\varrho) - \alpha \equiv 2^{t-2} \cdot \left(\xi + \sum_i z_i \frac{\partial \varphi(\xi_\varrho)}{\partial \xi_i}\right) \pmod{2^{t-1}}$$

d. h.

$$\varphi(x_\varrho) \equiv \alpha \pmod{2^{t-1}},$$

wenn man

$$\xi + \sum_i z_i \frac{\partial \varphi(\xi_\varrho)}{\partial \xi_i}$$

gerade macht. Dies lässt sich aber, da

$$\frac{\partial \varphi(\xi_\varrho)}{\partial \xi_i} = \frac{1}{2} \cdot \frac{\partial f(\xi_\varrho)}{\partial \xi_i}$$

ist, stets bewirken, wenn man für die Lösungen die Annahme macht, dass wenigstens eine der Zahlen (12) ungerade ist, dadurch dass man $n - 1$ der Zahlen z_ϱ (mod. 2) beliebig, eine gewisse derselben dagegen passend bestimmt. Somit erhält man mittels (14) zu jeder Wurzel der Congruenz (13), welche der Annahme genügt, genau 2^{n-1} solche Wurzeln der Congruenz (11), sodass die Anzahl der Wurzeln der gedachten Art für die letztere 2^{n-1} mal so gross ist, wie für die erstere. Ist daher A die Anzahl s o l c h e r Wurzeln der Congruenz

$$\varphi(x_\varrho) \equiv \alpha \pmod{2},$$

für welche nicht die sämmtlichen Ausdrücke (12) gerade sind, so ist die Anzahl ebensolcher Wurzeln für die Congruenz (11) gleich $\mathsf{A} \cdot 2^{(n-1)(t-2)}$. Auf die Congruenz (10) bezogen spricht sich dies Resultat in folgendem Satze aus:

Ist $2^n \cdot \mathsf{A} = 2^{n-1} \cdot 2\mathsf{A}$ die Anzahl der bezeichneten Wurzeln für die Congruenz

$$f(x_\varrho) \equiv 2\alpha \pmod{4}$$

so ist sie für die Congruenz

$$f(x_\varrho) \equiv 2\alpha \pmod{2^t}$$

gleich $2A \cdot 2^{(n-1)(t-1)}$.

Den vorstehenden drei Sätzen zufolge haben wir für den Fall, dass α nicht durch p resp. durch 2 theilbar ist, nur noch mit den Congruenzen:

$$f(x_\varrho) \equiv \alpha \pmod{p}$$

resp., jenachdem $f(x_\varrho)$ eine ungerade oder eine gerade Form ist, mit der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{8} \text{ oder } f(x_\varrho) \equiv 2\alpha \pmod{4}$$

zu thun.

2. Wie beschaffen nun α auch sei, so leuchtet ein, dass die Anzahl der Wurzeln der Congruenz

$$(15) \qquad f(x_\varrho) \equiv \alpha \pmod{q^t}$$

sich nicht ändert, wenn man $f(x_\varrho)$ durch irgend eine äquivalente Form $f'(y_\varrho)$ ersetzt, denn, wenn jene in diese übergeht durch die Substitution

$$x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho n} y_n, \quad (\varrho = 1, 2, \cdots n)$$

so entspricht vermöge der letzteren jeder Wurzel der Congruenz (15) eine Wurzel der Congruenz

$$(16) \qquad f'(y_\varrho) \equiv \alpha \pmod{q^t}$$

und umgekehrt. Offenbar darf hier aber auch $f'(y_\varrho)$ durch irgend eine andere quadratische Form ersetzt werden, deren Coefficienten den entsprechenden jener Form congruent sind. Und so darf man endlich, ohne dass die gesuchte Anzahl der Wurzeln der Congruenz sich ändert, an Stelle von $f(x_\varrho)$ in (15) irgend einen Hauptrest (mod. q^t) einsetzen und dadurch die Aufgabe auf eine wesentlich einfachere zurückführen*).

---

*) Man findet in Liouv. Journal 2. série t. 17 p. 368—402 eine Abhandlung von Camille Jordan, sur la forme canonique des congruences du second degré et le nombre de leurs solutions, in welcher

Wir behandeln nun zuerst den Fall, wo der Modulus eine ungerade Primzahl p ist. Ist dann o_m unter den Invarianten $o_1, o_2 \cdots o_{n-1}$ der Form $f(x_\varrho)$ die erste, welche durch p aufgeht, ω_m also die erste von Null verschiedene unter den Zahlen $\omega_1, \omega_2, \cdots \omega_{n-1}$, so folgt, wenn man in der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{p}$$

für $f(x_\varrho)$ einen Hauptrest (mod. p^t) setzt, nach Formel (25) vorigen Capitels folgende einfachere Congruenz:

$$(17) \qquad a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2 \equiv \alpha \pmod{p},$$

wo $a_1, a_2, \cdots a_m$ durch p nicht theilbare Zahlen bedeuten. Im Falle einer Primzahl p, welche nicht in der Determinante A der Form $f(x_\varrho)$ aufgeht, ist hierbei $m = n$. Um nun die Anzahl der Wurzeln der Congruenz (17) zu ermitteln, bemerken wir vor allem, dass sie für zwei verschiedene Werthe von α gleichviel Wurzeln hat, wenn dieselben gleichen quadratischen Charakter haben. Denn, sind α_1, α_2 zwei solche Werthe von α, so kann man

$$\alpha_1 \equiv \alpha_2 r^2, \quad \alpha_2 \equiv \alpha_1 s^2$$

setzen und aus jeder Lösung η_ϱ der Congruenz

$$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2 \equiv \alpha_1 \pmod{p}$$

erhält man eine Lösung $s\eta_\varrho$ der Congruenz

$$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2 \equiv \alpha_2,$$

und umgekehrt aus jeder Lösung η_ϱ der letzteren eine Lösung $r\eta_\varrho$ der erstgenannten Congruenz. Es bezeichne N_m die Anzahl der Wurzeln der Congruenz für einen quadratischen Rest

---

eine Methode entwickelt wird, um die Anzahl der Wurzeln der Congruenzen von der Gestalt:

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_m x_m^2 + b_{12} x_1 x_2 + \cdots \equiv c \pmod{M}$$

in jedem Falle zu finden. Diese Methode besteht im wesentlichen gleichfalls darin, dass der quadratischen Form ein Rest von „kanonischer Gestalt“ substituirt wird; aber da letztere von der hier als kanonisch gewählten abweicht, auch die quadratische Form selbst unter anderer Gestalt erscheint, so nimmt die Untersuchung insbesondere bezüglich des Moduls 2^t einen von dem hier dargestellten sehr verschiedenen Gang.

α, N'_m die Anzahl ihrer Wurzeln für einen quadratischen Nichtrest α; endlich sei N''_m die Anzahl der Wurzeln der Congruenz

(18) $$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2 \equiv 0 \pmod{p}.$$

Bedeutet dann F_m den Ausdruck

$$F_m = a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2$$

und ertheilt man in demselben den Zahlen $y_1, y_2, \cdots y_m$ alle möglichen Restwerthe (mod. p), was p^m Systeme $y_1, y_2, \cdots y_m$ ergiebt, so wird die Anzahl derjenigen dieser Systeme, für welche F_m ein quadratischer Rest wird, $\frac{p-1}{2} N_m$, die Anzahl derjenigen Systeme, für welche F_m ein quadratischer Nichtrest wird, $\frac{p-1}{2} N'_m$ sein und somit folgende erste Beziehung hervorgehen:

(19) $$p^m = N''_m + \frac{p-1}{2} \cdot (N_m + N'_m).$$

Die Wurzeln der Congruenz (18) lassen sich aber in zwei Arten vertheilen: diejenigen, bei welchen $y_m \equiv 0$ ist, deren Anzahl offenbar gleich der Anzahl der Wurzeln der Congruenz

$$F_{m-1} = a_1 y_1^2 + a_2 y_2^2 + \cdots + a_{m-1} y_{m-1}^2 \equiv 0 \pmod{p}$$

d. h. gleich N^0_{m-1} ist, und diejenigen, bei welchen y_m nicht durch p theilbar ist. Aus jeder der letzteren erhält man, wenn $a_m y_m^2$ nach rechts geschafft und mit der zu y_m^2 (mod. p) associirten Zahl multiplicirt wird, eine Wurzel der Congruenz

$$F_{m-1} \equiv -a_m \pmod{p}$$

und umgekehrt, sodass es $(p-1)N_{m-1}$ oder $(p-1)N'_{m-1}$ Wurzeln der zweiten Art giebt, jenachdem $\left(\frac{-a_m}{p}\right) = +1$ oder -1 ist. Je nach diesen beiden Fällen ist demnach

(20) $$\left\{\begin{array}{l} N''_m = N''_{m-1} + (p-1)N_{m-1} \\ \text{oder} \\ N''_m = N''_{m-1} + (p-1)N'_{m-1}. \end{array}\right.$$

Da zugleich

$$p^{m-1} = N''_{m-1} + \frac{p-1}{2}(N_{m-1} + N'_{m-1})$$

sein muss, so giebt die Verbindung der Formeln (19) und (20) leicht folgende neue Beziehung:

$$(21)\qquad 2p^{m-1} = N_m + N_m' + \left(\frac{-a_m}{p}\right)\cdot(N_{m-1} - N_{m-1}').$$

Wir verfolgen zunächst den Fall $m = 2$, betrachten also die Congruenz

$$(22)\qquad a_1 y_1^2 + a_2 y_2^2 \equiv \alpha \pmod{p}.$$

Der voraufgehenden allgemeinen Betrachtung zufolge bestehen die beiden Gleichungen

$$(23)\qquad p^2 = N_2^0 + \frac{p-1}{2}(N_2 + N_2')$$

und

$$(24)\qquad 2p = N_2 + N_2' + \left(\frac{-a_2}{p}\right)\cdot(N_1 - N_1');$$

N_1 bezeichnet dabei die Anzahl der Wurzeln der Congruenz

$$a_1 y_1^2 \equiv \alpha \pmod{p}$$

für einen quadratischen Rest α, N_1' für einen quadratischen Nichtrest α (mod. p), mithin findet sich sogleich

$$N_1 - N_1' = 2\cdot\left(\frac{a_1}{p}\right)$$

und die letzte Gleichung nimmt dadurch die Gestalt an

$$(25)\qquad 2p = N_2 + N_2' + 2\cdot\left(\frac{-a_1 a_2}{p}\right).$$

Nun sieht man zunächst leicht ein, dass N_2, N_2' von Null verschieden sind. Denn, wenn α ein quadratischer Rest ist, so wird (22), falls a_1 quadratischer Rest ist, für zwei Werthe von y_1 und für $y_2 \equiv 0$ (mod. p) gelöst; im entgegengesetzten Falle lässt die Differenz $\alpha - a_1 y_1^2$, während y_1 sämmtliche Werthe (mod. p) durchläuft, $\frac{p+1}{2}$ nicht durch p theilbare Reste (mod. p), unter denen also mindestens ein quadratischer Rest und ein quadratischer Nichtrest vorhanden ist, für welchen dann, jenachdem a_2 quadratischer Rest resp. Nichtrest ist, die Congruenz

$$a_2 y_2^2 \equiv \alpha - a_1 y_1^2 \pmod{p}$$

auflösbar ist. Somit muss jedenfalls N_2 von Null verschieden sein, und aus gleichen Erwägungen auch N_2'.

Dies vorausgeschickt, betrachten wir die Congruenzen

$$\left.\begin{array}{ll}(26) & a_1 y_1^2 + a_2 y_2^2 \equiv \alpha \\ (27) & a_1 y_1'^2 + a_2 y_2'^2 \equiv \alpha'\end{array}\right\} \pmod{p}.$$

Wenn sie erfüllt sind, so ist es auch die dritte:

$$(28) \qquad a_1 z_1^2 + a_2 z_2^2 \equiv a_1 \alpha\alpha' \pmod{p},$$

in welcher

$$z_1 \equiv a_1 y_1 y_1' + a_2 y_2 y_2', \quad z_2 \equiv a_1(y_1 y_2' - y_2 y_1')$$

ist, und man übersieht sogleich, dass incongruenten Lösungen einer der Congruenzen (26), (27) auch incongruente Lösungen von (28) entsprechen. Haben demnach α, α' verschiedenen quadratischen Charakter, so folgen aus den sämmtlichen Wurzeln derjenigen der Congruenzen (26), (27), deren rechte Seite mit a_1 gleichen quadratischen Charakter hat, zusammen mit einer Wurzel der anderen von ihnen ebenso viel verschiedene Wurzeln der Congruenz (28), deren rechte Seite alsdann einen von a_1 verschiedenen Charakter hat, woraus hervorgeht, dass eine der beiden Zahlen N_2, N_2' der anderen mindestens gleich ist. Wählt man ein anderes Mal α, α' beide von demselben aber zu dem von a_1 entgegengesetzten Charakter, so folgen aus den sämmtlichen Wurzeln der Congruenz (26) zusammen mit einer Wurzel von (27) ebenso viel verschiedene Wurzeln der Congruenz (28), deren rechte Seite jetzt gleichen quadratischen Charakter hat wie a_1, und daraus folgt jetzt, dass die andere der Zahlen N_2, N_2' der ersteren mindestens gleich ist. Beides zusammen lehrt die Gleichheit

$$N_2 = N_2'.$$

Infolge dieses Resultates ergiebt nun sofort die Formel (25) die Werthe

$$(29) \qquad N_2 = N_2' = p - \left(\frac{-a_1 a_2}{p}\right),$$

während

$$(30) \qquad N_2^0 = p + (p-1)\cdot\left(\frac{-a_1 a_2}{p}\right)$$

gefunden wird. —

Setzt man nunmehr

$$F_{m-2} = a_1 y_1^2 + a_2 y_2^2 + \cdots + a_{m-2} y_{m-2}^2$$

die Congruenz (17) also in die Gestalt:

$$a_{m-1}y_{m-1}^2 + a_m y_m^2 \equiv \alpha - F_{m-2} \pmod{p},$$

so kann man ihre Wurzeln in diejenigen unterscheiden, für welche

$$F_{m-2} \equiv \alpha \pmod{p}$$

ist, und diejenigen, welche diese Congruenz nicht erfüllen. Ist zunächst α ein quadratischer Rest (mod. p), so giebt es N_{m-2} Systeme $y_1, y_2, \cdots y_{m-2}$ der ersteren Art und jedem von ihnen entsprechen nach der soeben entwickelten Theorie — wobei nur a_1, a_2 durch a_{m-1}, a_m zu ersetzen sind —

$$p + (p-1) \cdot \left(\frac{-a_{m-1}a_m}{p}\right)$$

Systeme y_{m-1}, y_m; jedem der $p^{m-2} - N_{m-2}$ übrigen Restsysteme $y_1, y_2, \cdots y_{m-2}$ (mod. p) aber entsprechen

$$p - \left(\frac{-a_{m-1}a_m}{p}\right)$$

Systeme y_{m-1}, y_m. Im Ganzen also findet sich die Anzahl der incongruenten Systeme $y_1, y_2, \cdots y_m$, welche der Congruenz (17) genügen,

$$N_m = \left[p + (p-1)\left(\frac{-a_{m-1}a_m}{p}\right)\right] \cdot N_{m-2}$$
$$+ \left[p - \left(\frac{-a_{m-1}a_m}{p}\right)\right](p^{m-2} - N_{m-2})$$

d. i.

$$N_m = p^{m-2}\left(p - \left(\frac{-a_{m-1}a_m}{p}\right)\right) + N_{m-2} \cdot p \cdot \left(\frac{-a_{m-1}a_m}{p}\right).$$

Ganz ebenso führt die Annahme, dass α ein quadratischer Nichtrest sei, zur Beziehung

$$N'_m = p^{m-2}\left(p - \left(\frac{-a_{m-1}a_m}{p}\right)\right) + N'_{m-2} \cdot p \cdot \left(\frac{-a_{m-1}a_m}{p}\right)$$

und folglich erhält man auch diese andere:

$$(31) \qquad N_m - N'_m = (N_{m-2} - N'_{m-2}) \cdot p \cdot \left(\frac{-a_{m-1}a_m}{p}\right).$$

Aus gleichen Gründen bestehen aber die ähnlichen Gleichungen:

$$N_{m-2} - N'_{m-2} = (N_{m-4} - N'_{m-4}) \cdot p \cdot \left(\frac{-a_{m-3}a_{m-2}}{p}\right)$$

u. s. w., aus deren Combination sich endlich

für ein gerades m wegen der Gleichheit

$$N_2 = N_2'$$

auch

$$N_m = N_m', \tag{32}$$

dagegen für ein ungerades m wegen

$$N_1 - N_1' = 2 \cdot \left(\frac{a_1}{p}\right)$$

die Formel

$$N_m - N_m' = 2p^{\frac{m-1}{2}} \cdot \left(\frac{(-1)^{\frac{m-1}{2}} a_1 a_2 \cdots a_m}{p}\right) \tag{33}$$

ergiebt.

Verbindet man nun mit einander die Formeln (21) und (32) resp. (33), so gewinnt man ohne Mühe folgende Werthe:

für ein gerades m:

$$\begin{cases} N_m = N_m' = p^{m-1} - p^{\frac{m}{2}-1} \cdot \left(\frac{(-1)^{\frac{m}{2}} a_1 a_2 \cdots a_m}{p}\right) \\ N_m'' = p^{m-1} + (p-1)p^{\frac{m}{2}-1} \cdot \left(\frac{(-1)^{\frac{m}{2}} a_1 a_2 \cdots a_m}{p}\right); \end{cases} \tag{34a}$$

für ein ungerades m:

$$\begin{cases} N_m = p^{m-1} + p^{\frac{m-1}{2}} \cdot \left(\frac{(-1)^{\frac{m-1}{2}} a_1 a_2 \cdots a_m}{p}\right) \\ N_m' = p^{m-1} - p^{\frac{m-1}{2}} \cdot \left(\frac{(-1)^{\frac{m-1}{2}} a_1 a_2 \cdots a_m}{p}\right) \\ N_m'' = p^{m-1}. \end{cases} \tag{34b}$$

Nach diesen Formeln kann in jedem Falle die Anzahl der Wurzeln angegeben werden, welche die Congruenz (17) besitzt. Für den Fall, dessen wir in der Folge besonders bedürfen, in welchem α nicht durch p theilbar ist, findet sich so der Satz:

Die Congruenz (17), in welcher α nicht $\equiv 0 \pmod{p}$ ist, hat, wenn m *gerade* ist,

$$p^{m-1} - p^{\frac{m}{2}-1} \cdot \left(\frac{(-1)^{\frac{m}{2}} a_1 a_2 \cdots a_m}{p}\right) \tag{35a}$$

und, wenn *m ungerade* ist,

$$(35\text{b}) \qquad p^{m-1} + p^{\frac{m-1}{2}} \cdot \left(\frac{(-1)^{\frac{m-1}{2}} a_1 a_2 \cdots a_m \alpha}{p} \right)$$

verschiedene Wurzeln*).

Bedenkt man aber, dass diejenigen $n - m$ Unbestimmten der Congruenz

$$f'(y_\varrho) \equiv \alpha \pmod{p},$$

welche nicht in (17) verbleiben, jeden beliebigen Werth (mod. p) erhalten dürfen, so folgt hieraus, dass die Anzahl Wurzeln der Congruenz

---

*) Dies Resultat findet man bewiesen in C. Jordan's traité des substitutions p. 159; es wird dort — scheinbar einfacher — mittels allgemeiner Induktion erschlossen, giebt aber damit nicht die rechte Einsicht in die Gründe, auf denen der Satz beruht. Wir haben daher vorgezogen, uns — im wesentlichen — den Gesichtspunkten anzuschliessen, deren Lebesgue in seinen recherches sur les nombres § 5 in Liouv. Journal t. 2 p. 266—275 gefolgt ist. Diese interessante Arbeit enthält eine Methode zur Bestimmung der Anzahl der Wurzeln der Congruenz

$$a_1 x_1^m + a_2 x_2^m + \cdots a_\varkappa x_\varkappa^m \equiv a_{\varkappa+1} \pmod{p = mh + 1}$$

und giebt als einfachste Anwendung derselben die Anzahl der Wurzeln der Congruenz

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_\varkappa x_\varkappa^2 \equiv a_{\varkappa+1} \pmod{p = 2h + 1};$$

als fernere Beispiele aber behandelt Lebesgue auch die zwei Congruenzen

$$a_1 x_1^3 + a_2 x_2^3 \equiv a_3 \pmod{p = 3h + 1}$$

und

$$a_1 x_1^4 + a_2 x_2^4 \equiv a_3 \pmod{p = 4h + 1}$$

und leitet dabei die berühmten Sätze her, welche die Reste der Ausdrücke

$$\left.\begin{array}{c} \dfrac{2h(2h-1)\cdots(h+1)}{1\cdot 2\cdots h} \\ \text{resp.} \\ \dfrac{1}{2}\cdot\dfrac{2h(2h-1)\cdots(h+1)}{1\cdot 2\cdots h} \end{array}\right\} \pmod{p}$$

mit der Zerlegung der Zahl p beziehungsweise in die Formen

$$L^2 + 27M^2 = 4p, \quad L^2 + M^2 = p$$

in Verbindung setzen. (S. meine Lehre von der Kreistheilung S. 143, 144 resp. S. 137.)

(36) $$f(x_\varrho) \equiv \alpha \pmod{p},$$

wenn die erste durch p theilbare Invariante

$$o_1, o_2, \cdots o_{n-1}$$

von *geradem* Index m ist,

$$A = p^{n-1} \cdot \left[1 - p^{-\frac{m}{2}} \cdot \left(\frac{(-1)^m a_1 a_2 \cdots a_m}{p}\right)\right],$$

wenn sie von *ungeradem* Index m ist,

$$A = p^{n-1} \cdot \left[1 + p^{-\frac{m-1}{2}} \cdot \left(\frac{(-1)^{\frac{m-1}{2}} a_1 a_2 \cdots a_m \alpha}{p}\right)\right]$$

ist. Aus der Congruenz (25) vorigen Capitels ergiebt sich

$$\sigma_m d_{m-1} \cdot f'_m \equiv a_1 a_2 \cdots a_m \pmod{p};$$

also hangt das Legendre'sche Symbol, welches die vorstehenden Formeln enthalten, und somit auch die Anzahl der Wurzeln der Congruenz (36) ausser von α und von der Ordnung der Form $f(x_\varrho)$ ausschliesslich von dem auf die Primzahl p bezüglichen Charakter $\left(\frac{f'_m}{p}\right)$ derselben ab, und auch umgekehrt kann dieser Charakter der Form aus der Anzahl der Wurzeln der Congruenz (36) mittels jener Formeln erschlossen werden. Die Anzahl der Congruenzwurzeln bezüglich einer nicht in der Determinante aufgehenden Primzahl p ist unabhängig vom Geschlecht nur durch die Ordnung der Form bestimmt. Denn in diesem Falle geht das Symbol $\left(\frac{a_1 a_2 \cdots a_m}{p}\right)$ in das folgende

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{A}{p}\right)$$

über.

3. Betrachten wir jetzt zweitens die Congruenz

(37) $$f(x_\varrho) \equiv \alpha \pmod{8}$$

für den Fall, dass α eine ungerade Zahl und $f(x_\varrho)$ eine ungerade Form ist. Wir dürfen letztere durch einen Hauptrepräsentanten $f'(y_\varrho)$ (mod. 2^t) und diesen durch seinen Rest ersetzen und erhalten, wenn wir uns auf den Fall beschränken, dass die Determinante A der Form ungerade ist, statt der

Congruenz

(38) $$f'(y_\varrho) \equiv \alpha \pmod{8}$$

nach (31) vorigen Capitels eine Congruenz von der Gestalt:

(39) $$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2 \equiv \alpha \pmod{8},$$

wo $a_1, a_2, \cdots a_n$ ungerade Zahlen sind. Hierbei betrachte man nur solche Wurzeln derselben, bei denen nicht sämmtliche y_i ungerade sind. Jede solche Wurzel $y_1, y_2, \cdots y_n$ ist nun auch eine Wurzel derselben Congruenz (mod. 4); ist aber etwa y_1 gerade, so stellen auch

$$y_1 + 2,\ y_2,\ \cdots y_n$$

eine solche dar, für welche jedoch

(39a) $$a_1 (y_1 + 2)^2 + a_2 y_2^2 + \cdots + a_n y_n^2 \equiv \alpha + 4 \pmod{8}$$

ist. Die bezeichneten Wurzeln der Congruenz

(40) $$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2 \equiv \alpha \pmod{4}$$

lassen sich also in Paare so vertheilen, dass der einen Wurzel jeden Paares eine Lösung der Congruenz (39), der andern eine solche der Congruenz (39a) entspricht; da jedoch aus einer Lösung $y_1, y_2, \cdots y_n$ von (39) resp. (39a), wenn man die y_i um 4 verändert, genau 2^n Wurzeln derselben entspringen, so wird die Anzahl A der bezeichneten Wurzeln von (39) gleich $2^n \cdot \frac{1}{2} \mathfrak{A}$ sein, unter $\mathfrak{A}$ die Anzahl der bezeichneten Wurzeln verstanden, welche der Congruenz (40) eigen sind, man hat mithin

(41) $$\mathsf{A} = 2^{n-1} \cdot \mathfrak{A}.$$

Um nun $\mathfrak{A}$ zu bestimmen, bemerke man, dass die Congruenz (40) keine Lösungen in lauter ungeraden Zahlen haben kann, wenn n gerade, oder auch, wenn n ungerade und

$$a_1 + a_2 + \cdots + a_n \equiv -\alpha \pmod{4}$$

ist; dagegen 2^n solche Wurzeln, wenn n ungerade und

$$a_1 + a_2 + \cdots + a_n \equiv \alpha \pmod{4}$$

ist. Da man aber $\mathfrak{A}$ findet, wenn man die Anzahl der Wurzeln in lauter ungeraden Zahlen von der Anzahl aller Wurzeln der Congrueuz (40) überhaupt abzieht, erübrigt nur, diese Anzahl ihrer sämmtlichen Wurzeln zu finden.

Letztere Aufgabe soll nun unter der allgemeineren Voraussetzung eines beliebigen α gelöst werden. Man nehme an, von den Coefficienten $a_1, a_2, \cdots a_n$ seien μ von der Form $4j+1$, ν von der Form $4j+3$, sodass $\mu+\nu=n$ ist; mit η bezeichne man den kleinsten positiven Rest von α (mod. 4). Die Congruenz (40) ist dann der folgenden:

$$(42) \quad z_1^2+z_2^2+\cdots+z_\mu^2-(u_1^2+u_2^2+\cdots+u_\nu^2)\equiv\eta \pmod{4}$$

gleichbedeutend. Man sieht sogleich, dass eine Congruenz

$$(43) \qquad z_1^2+z_2^2+\cdots+z_\mu^2\equiv\eta \pmod{4}$$

nur dann erfüllt wird, wenn von den μ Zahlen $z_1, z_2, \cdots z_\mu$ eine Anzahl $s=4h+\eta$ ungerade, die übrigen gerade gewählt werden, und dass man so jedesmal 2^μ Wurzeln der Congruenz erhält. Setzt man also

$$M_\eta = 2^\mu \cdot \sum_{s=4h+\eta} \frac{\mu(\mu-1)\cdots(\mu-s+1)}{1\cdot 2\cdots s},$$

indem man diese Summation auf alle Zahlen s der genannten Form erstreckt, welche $\overline{\gtrless}\ \mu$ sind, so bezeichnet M_η die Anzahl der Wurzeln von (43). Nun besteht aber folgende Entwickelung:

$$2^\mu\cdot(1+i^\varrho)^\mu = M_0+i^\varrho M_1+i^{2\varrho}M_2+i^{3\varrho}M_3;$$

und, wenn man analog

$$N_\eta = 2^\nu \cdot \sum_{s=4h+\eta} \frac{\nu(\nu-1)\cdots(\nu-s+1)}{1\cdot 2\cdots s}$$

setzt und die Summation über die angedeuteten $s\ \overline{\gtrless}\ \nu$ erstreckt, so bezeichnet gleicherweise N_η die Anzahl der Wurzeln der Congruenz

$$u_1^2+u_2^2+\cdots+u_\nu^2\equiv\eta \pmod{4}$$

und es ist

$$2^\nu\cdot(1+i^{3\varrho})^\nu = N_0+i^{3\varrho}N_1+i^{2\varrho}N_2+i^\varrho N_3.$$

Durch Multiplikation dieser beiden Formeln mit einander ergiebt sich

$$(44) \quad 2^n\cdot(1+i^\varrho)^\mu\cdot(1+i^{3\varrho})^\nu = P_0+i^\varrho P_1+i^{2\varrho}P_2+i^{3\varrho}P_3,$$

wenn zur Abkürzung

$$M_0N_0 + M_1N_1 + M_2N_2 + M_3N_3 = P_0$$
$$M_0N_3 + M_1N_0 + M_2N_1 + M_3N_2 = P_1$$
$$M_0N_2 + M_1N_3 + M_2N_0 + M_3N_1 = P_2$$
$$M_0N_1 + M_1N_2 + M_2N_3 + M_3N_0 = P_3$$

geschrieben wird. Offenbar bezeichnen aber diese so (für $\eta = 0, 1, 2, 3$) definirten Zahlen P_η die Anzahl der Wurzeln der Congruenz (42) oder (40); denn z. B. für $\eta = 1$ erhält man die Wurzeln dieser Congruenz, wenn man die Quadratsummen

$$z_1^2 + z_2^2 + \cdots + z_\mu^2, \quad u_1^2 + u_2^2 + \cdots + u_\nu^2$$

resp. congruent 1, 0 oder 2, 1 oder 3, 2 oder 0, 3 (mod. 4) macht, was je auf $M_1 \cdot N_0$, $M_2 \cdot N_1$, $M_3 \cdot N_2$, $M_0 \cdot N_3$ Weisen geschehen kann, u. s. w. Setzt man folglich

$$P_0 + i^\varrho P_1 + i^{2\varrho} P_2 + i^{3\varrho} P_3 = \varpi_\varrho,$$

so erhält man die gesuchte Anzahl der Wurzeln durch die Formel

$$(45) \qquad 4 \cdot P_\eta = \varpi_0 + i^{3\eta}\varpi_1 + i^{2\eta}\varpi_2 + i^\eta \varpi_3.$$

Nun ist nach (44)

$$(46) \quad \begin{cases} \varpi_0 = 2^{2n}, \; \varpi_2 = 0 \\ \varpi_1 = 2^n(1+i)^\mu(1-i)^\nu = 2^n(1+i)^n \cdot (-i)^\nu \\ \varpi_3 = 2^n(1-i)^\mu(1+i)^\nu = 2^n(1-i)^n \cdot i^\nu. \end{cases}$$

Die letzteren Formeln lassen noch eine beträchtliche Umgestaltung zu. Setzt man, indem man durch $[a]$ das grösste Ganze von a ausdrückt,

$$\left[\frac{n}{2}\right] = 2 \cdot \left[\frac{n}{4}\right] + r, \quad \nu = 2 \cdot \left[\frac{\nu}{2}\right] + \lambda,$$

wo r und λ einen der Werthe 0, 1 haben müssen, so kann man wegen der Gleichheit

$$\left(\frac{1+i}{\sqrt{2}}\right)^2 = i$$

die Formel für ϖ_1 auch so schreiben:

$$\varpi_1 = 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot i^{\left[\frac{n}{2}\right]+3\nu}$$
$$= 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot (-1)^{\left[\frac{n}{4}\right]+\left[\frac{\nu}{2}\right]} \cdot i^{r-\lambda}.$$

Ist nun $\left[\frac{n}{2}\right] \equiv \nu$ also $r \equiv \lambda$ (mod. 2), so muss auch $r = \lambda$ sein, dann wird also

$$\varpi_1 = 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot (-1)^{\left[\frac{n}{4}\right]+\left[\frac{\nu}{2}\right]}.$$

Ist dagegen $\left[\frac{n}{2}\right] \gtrless \nu$ (mod. 2), so muss $r + \lambda = 1$ sein, und da man schreiben darf

$$\varpi_1 = 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot (-1)^{\left[\frac{n}{4}\right]+\left[\frac{\nu}{2}\right]+\nu} \cdot i^{r+\lambda},$$

kommt einfacher

$$\varpi_1 = 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot (-1)^{\left[\frac{n}{4}\right]+\left[\frac{\nu}{2}\right]+\nu} \cdot i.$$

4. Hier führen wir folgende zwei Einheiten ein:

$$(47) \qquad \varepsilon = (-1)^{\left[\frac{n}{2}\right]+\nu}, \quad \delta = (-1)^{\left[\frac{n}{4}\right]+\left[\frac{\nu}{2}\right]} \cdot \varepsilon^{\left[\frac{n}{2}\right]}.$$

Bemerkt man dann, dass ϖ_1 und ϖ_3 conjugirt imaginär sind, so darf man sagen:

Ist $\varepsilon = +1$, so ist:

$$(48) \qquad \begin{cases} \varpi_1 = 2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot \delta \\ \varpi_3 = 2^{\frac{3n}{2}} \cdot \left(\frac{1-i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot \delta; \end{cases}$$

ist aber $\varepsilon = -1$, so ist:

$$(48a) \qquad \begin{cases} \varpi_1 = -2^{\frac{3n}{2}} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot \delta i \\ \varpi_3 = +2^{\frac{3n}{2}} \cdot \left(\frac{1-i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \cdot \delta i. \end{cases}$$

Durch Einführung der für die ϖ_ϱ gefundenen Werthe in die Formel (45) erhält man die gesuchten Zahlen P_η. Wir stellen sie, nach den möglichen Fällen, in folgender Tabelle zusammen:

I. n gerade.

Ist dann 1) $\varepsilon = +1$, so ist

$$4P_0 = 2^{2n} + \delta \cdot 2^{\frac{3n}{2}+1},\ 4P_2 = 2^{2n} - \delta \cdot 2^{\frac{3n}{2}+1}$$
$$4P_1 = 4P_3 = 2^{2n};$$

Ist 2) $\varepsilon = -1$, so ist

$$4P_1 = 2^{2n} - \delta \cdot 2^{\frac{3n}{2}+1},\ 4P_3 = 2^{2n} + \delta \cdot 2^{\frac{3n}{2}+1}$$
$$4P_0 = 4P_2 = 2^{2n}.$$

II. n **ungerade.**

Ist dann 1) $\varepsilon = +1$, so ist

$$4P_0 = 4P_1 = 2^{2n} + \delta \cdot 2^{\frac{3n+1}{2}},$$
$$4P_2 = 4P_3 = 2^{2n} - \delta \cdot 2^{\frac{3n+1}{2}};$$

Ist 2) $\varepsilon = -1$, so ist

$$4P_0 = 4P_3 = 2^{2n} + \delta \cdot 2^{\frac{3n+1}{2}},$$
$$4P_2 = 4P_1 = 2^{2n} - \delta \cdot 2^{\frac{3n+1}{2}}\ *).$$

Die Einheiten ε und δ müssen wir noch näher betrachten. Offenbar werden soviel der Coefficienten a_i congruent -1 (mod. 4) sein, als von den Zahlen $\frac{a_i - 1}{2}$ ungerade sind, und daraus folgt sogleich

$$(-1)^\nu = (-1)^{\sum_{i=1}^{n} \frac{a_i - 1}{2}};$$

noch einfacher wird, da nach der Congruenz

$$(49) \qquad f'(y_\varrho) \equiv a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2 \pmod{2^\ell}$$
$$A \equiv a_1 a_2 \cdots a_n \pmod{4}$$

ist,

$$(-1)^\nu = (-1)^{\frac{A-1}{2}}$$

und somit

---

*) Andere Ausdrücke hat Smith in seinem mém. sur la représentation etc. art. 8 gegeben; unterscheidet man die Fälle, in welchen n von den Formen $4j$, $4j+1$, $4j+2$, $4j+3$ ist, so bestätigt man durch die gefundenen Formeln leicht die dort angegebenen Smith-schen Ausdrücke für die von ihm durch das Zeichen Φ bezeichneten Funktionen.

(50) $$\varepsilon = (-1)^{\left[\frac{n}{2}\right]} \cdot (-1)^{\frac{A-1}{2}}$$

sein. Man bemerke auch zu späterer Verwendung, dass aus der Congruenz

$$a_1 + a_2 + \cdots + a_n \equiv \mu - \nu \equiv n + 2\nu \pmod{4}$$

für den Fall eines ungeraden n die folgende:

$$\frac{a_1 + a_2 + \cdots + a_n - 1}{2} \equiv \left[\frac{n}{2}\right] + \nu \pmod{2}$$

also

$$\varepsilon = (-1)^{\frac{\varepsilon-1}{2}} = (-1)^{\frac{a_1+a_2+\cdots+a_n-1}{2}}$$

und folglich

(50a) $$\varepsilon \equiv a_1 + a_2 + \cdots + a_n \pmod{4}$$

sich ergiebt.

Ferner werden unter den $\frac{n(n-1)}{2}$ Produkten

$$\frac{a_i - 1}{2} \cdot \frac{a_k - 1}{2},$$

welche verschiedenen Indices i, k entsprechen, genau so viel ungerade sein, als die ν verschiedenen Indices, denen Coefficienten a_i, a_k von der Form $4j + 3$ entsprechen, zu zweien combinirt werden können, d. h. $\frac{\nu(\nu-1)}{2}$, und man findet sogleich, da offenbar

$$\frac{\nu(\nu-1)}{2} \equiv \left[\frac{\nu}{2}\right] \pmod{2}$$

ist,

$$(-1)^{\left[\frac{\nu}{2}\right]} = (-1)^{\frac{\nu(\nu-1)}{2}} = (-1)^{\sum \frac{a_i-1}{2} \cdot \frac{a_k-1}{2}},$$

die Summation auf alle $\frac{n(n-1)}{2}$ Combinationen zu zwei verschiedenen Indices der Reihe $1, 2, 3, \cdots n$ bezogen. Der Exponent dieser Potenz von -1 ist aber (mod. 2) mit dem folgenden:

$$\frac{a_1 - 1}{2} \cdot \frac{a_2 - 1}{2} + \frac{a_1 a_2 - 1}{2} \cdot \frac{a_3 - 1}{2} + \cdots$$
$$+ \frac{a_1 a_2 \cdots a_{n-1} - 1}{2} \cdot \frac{a_n - 1}{2}$$

oder auch, wie man leicht übersieht, mit diesem anderen:

$$(51) \qquad \sum_{m=1}^{n-1} \frac{a_1 a_2 \cdots a_m - 1}{2} \cdot \frac{a_1 a_2 \cdots a_{m+1} + 1}{2}$$

congruent. Nun folgt aber, da die Invarianten σ_m der Form $f'(y_\varrho)$ sämmtlich gleich 1 sind, aus (49) die Beziehung

$$d_{m-1} \cdot f'_m \equiv a_1 a_2 \cdots a_m \pmod{4},$$

und daher ist das allgemeine Glied der vorstehenden Summe mit folgendem Ausdrucke

$$\frac{d_{m-1} \cdot f'_m - 1}{2} \cdot \frac{d_m \cdot f'_{m+1} + 1}{2}$$

(mod. 2) congruent, welchem, wenn man die aus der Beziehung

$$d_{m-1}^2 \cdot o_m = d_m \cdot d_{m-2}$$

fliessende Congruenz

$$o_m \equiv d_m \cdot d_{m-2} \pmod{4}$$

benutzt, der andere (mod. 2) substituirt werden darf:

$$\frac{1}{4}[(d_{m-1} - 1)(d_m + 1) + (d_{m-2} - 1)(f'_m - 1) \\ + (d_{m-1} - 1)(f'_{m+1} - 1)] \\ + \frac{o_m + 1}{2} \cdot \frac{f'_m - 1}{2} + \frac{f'_m - 1}{2} \cdot \frac{f'_{m+1} - 1}{2}.$$

Demnach findet sich die ganze Summe (51) (mod. 2) congruent mit folgendem Ausdrucke:

$$\sum_{m=1}^{n-1} \frac{1}{4}(d_{m-1} - 1)(d_m + 1) + \frac{1}{2}(d_{n-2} - 1)\tau \\ + \sum_{m=1}^{n-1} \left(\frac{o_m + 1}{2} \cdot \frac{f'_m - 1}{2} + \frac{f'_m - 1}{2} \cdot \frac{f'_{m+1} - 1}{2} \right)$$

d. i., da hier die Grössen o_m mit den durch e_m benannten identisch sind, mit dem einfachen Ausdrucke:

$$\frac{1}{2}(d_{n-2} - 1)\tau + \sum_{m=1}^{n-1} \frac{1}{4}(d_{m-1} - 1)(d_m + 1) + \psi(o, n-1).$$

Auf solche Weise geht der Ausdruck für die Einheit δ in nachstehenden über:

$$(52) \qquad \delta = (-1)^{\left[\frac{n}{4}\right] + \sigma + \psi(o, n-1)} \cdot \varepsilon^{\left[\frac{n}{2}\right]},$$

wo

$$(52\text{a})\qquad \sigma = \frac{1}{4}(d_1 - 1)(d_2 + 1) + \frac{1}{4}(d_2 - 1)(d_3 + 1) + \cdots$$
$$+ \frac{1}{4}(d_{n-3} - 1)(d_{n-2} + 1)$$
$$+ \frac{1}{4}(d_{n-2} - 1)(\Delta + 1)$$

ist. Die Einheit ε hangt somit nur von der Ordnung, die Einheit δ ausser von der Ordnung der Form $f(x_\varrho)$ auch von ihrem Simultancharakter $(-1)^{\psi(0,n-1)}$ ab.

Demnach wird auch die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{8}$$

ausser durch die Ordnung der Form $f(x_\varrho)$ nur durch ihren Simultancharakter $(-1)^{\psi(0,n-1)}$ bestimmt, den sie auch ihrerseits umgekehrt definirt.

Mit ε_1, δ_1 mögen noch die Einheiten bezeichnet werden, welche sich auf die quadratische Form

$$a_2 y_2^2 + a_3 y_3^2 + \cdots + a_n y_n^2$$

auf gleiche Weise beziehen, wie ε, δ auf die Form

$$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2;$$

es seien also

$$\varepsilon_1 = (-1)^{\left[\frac{n-1}{2}\right] + \nu_1},$$

wo ν_1 die Anzahl derjenigen unter den Zahlen

$$a_2, a_3, \cdots a_n$$

ist, welche die Form $4j + 3$ haben, und

$$\delta_1 = (-1)^{\left[\frac{n-1}{4}\right] + \left[\frac{\nu_1}{2}\right]} \cdot \varepsilon_1^{\left[\frac{n-1}{2}\right]}.$$

Wenn man bedenkt, dass, jenachdem a_1 von der Form $4j + 1$ oder $4j + 3$ ist, $\nu_1 = \nu$ oder $\nu_1 = \nu - 1$ ist, und wenn man die leicht ersichtlichen Congruenzen

$$\left.\begin{aligned} \left[\frac{n-1}{2}\right] &\equiv \left[\frac{n}{2}\right] + n - 1 \\ \left[\frac{n-1}{4}\right] &\equiv \left[\frac{n}{4}\right] + (n-1) \cdot \left[\frac{n-1}{2}\right] \end{aligned}\right\} \pmod{2}$$

benutzt, so finden sich ohne Mühe die beiden Gleichungen:

$$(53)\qquad \begin{cases} \varepsilon_1 = (-1)^{n-1+\frac{a_1-1}{2}} \cdot \varepsilon \\ \delta_1 = (-1)^{n\cdot\frac{a_1-1}{2}} \cdot \varepsilon^{n-1+\frac{a_1-1}{2}} \cdot \delta, \end{cases}$$

durch welche die Einheiten ε_1, δ_1 auf die anderen ε, δ zurückgeführt werden.

5. Wir behandeln endlich drittens die Congruenz

$$(54)\qquad f(x_\varrho) \equiv 2\alpha \pmod{4},$$

in welcher $f(x_\varrho)$ eine gerade Form sein soll, jedoch wollen wir auch hier uns auf den Fall beschränken, wo die Determinante der letzteren ungerade ist, was n gerade voraussetzt; es leuchtet ein, dass dann diejenigen Auflösungen, für welche sämmtliche Ausdrücke (12) gerade sind, die geraden Auflösungen der Congruenz sein werden, solche also nicht vorhanden sind, sobald α ungerade gedacht wird. Der Congruenz (54) kann man die andere

$$f'(y_\varrho) \equiv 2\alpha \pmod{4},$$

in welcher $f'(y_\varrho)$ irgend einen Hauptrepräsentanten (mod. 2^{t_0}) der Classe von f bezeichnet, und dieser nach der Formel (40) des vorigen Capitels eine Congruenz von folgender Gestalt substituiren:

$$(55)\qquad \sum_{i=1}^{m} 2(a_i x^2 + \mathfrak{A}_i xy + \mathfrak{a}_i y^2) \equiv 2\alpha \pmod{4},$$

in welcher a_i, $\mathfrak{A}_i$ ungerade Zahlen und m die Zahl $\frac{n}{2}$ bedeuten.

Wir untersuchen zunächst für ein beliebiges α, wieviel Wurzeln eine Congruenz von der Form

$$a_i x^2 + \mathfrak{A}_i xy + \mathfrak{a}_i y^2 \equiv \alpha \pmod{2}$$

hat. Ist α ungerade, so muss, wenn

$$\mathfrak{a}_i \text{ gerade d. i. } 4a_i\mathfrak{a}_i - \mathfrak{A}_i^2 \equiv 7 \pmod{8} \text{ ist,}$$

x ungerade, y gerade gewählt werden, also ist nur eine Wurzel (mod. 2) vorhanden; ist aber

$$\mathfrak{a}_i \text{ ungerade d. i. } 4a_i\mathfrak{a}_i - \mathfrak{A}_i^2 \equiv 3 \pmod{8},$$

so kann y gerade und x ungerade, oder y ungerade und x beliebig gewählt werden, also sind drei Wurzeln (mod. 2)

vorhanden. Umgekehrt wird sich's verhalten, wenn α gerade ist.

Dies vorausgeschickt, bezeichne man mit μ die Anzahl der m Ausdrücke

(56) $$a_i x^2 + \mathfrak{A}_i xy + \mathfrak{a}_i y^2,$$

für welche der erste Fall statthat d. h. für welche

$$\left(\frac{2}{4a_i\mathfrak{a}_i - \mathfrak{A}_i^2}\right) = +1$$

ist, mit ν die Anzahl derjenigen, für welche dies Symbol gleich -1 ist, sodass $\mu + \nu = m$ ist.

Wenn nun zunächst α gerade ist, so hat man in (55) eine gerade Anzahl der Ausdrücke (56) also

entweder $2h$ der μ Ausdrücke und $2\varkappa$ der ν Ausdrücke
oder $2h+1$ „ „ „ „ $2\varkappa+1$ „ „ „

von dieser Gestalt ungerade, die übrigen gerade zu machen, was

im ersten Falle $3^{\mu-2h}\cdot 3^{2\varkappa}$
im zweiten Falle $3^{\mu-2h-1}\cdot 3^{2\varkappa+1}$

Wurzeln der Congruenz

(57) $$\sum_{i=1}^{m}(a_i x^2 + \mathfrak{A}_i xy + \mathfrak{a}_i y^2) \equiv \alpha \pmod{2}$$

ergiebt. Man erhält die Gesammtzahl der Wurzeln dieser Congruenz, wenn man die gedachte Auswahl auf alle möglichen Weisen trifft und die ihnen entsprechenden Zahlen addirt; so findet sie sich offenbar gleich

$$\sum_h \frac{\mu(\mu-1)\cdots(\mu-2h+1)}{1\cdot 2\cdots 2h}\cdot 3^{\mu-2h}\cdot\sum_\varkappa \frac{\nu(\nu-1)\cdots(\nu-2\varkappa+1)}{1\cdot 2\cdots 2\varkappa}\cdot 3^{2\varkappa}$$

$$+\sum_h \frac{\mu(\mu-1)\cdots(\mu-2h)}{1\cdot 2\cdots(2h+1)}\cdot 3^{\mu-2h-1}\cdot\sum_\varkappa \frac{\nu(\nu-1)\cdots(\nu-2\varkappa)}{1\cdot 2\cdots(2\varkappa+1)}\cdot 3^{2\varkappa+1}$$

$$=\frac{1}{4}[(3+1)^\mu + (3-1)^\mu]\cdot[(1+3)^\nu + (1-3)^\nu]$$

$$+\frac{1}{4}[(3+1)^\mu - (3-1)^\mu]\cdot[(1+3)^\nu - (1-3)^\nu]$$

oder, vereinfacht, gleich

$$2^{2m-1}\cdot\left(1+\frac{(-1)^{\nu}}{2^m}\right).$$

Nun ist $2m = n$ und offenbar $(-1)^{\nu} = \Theta$, wenn wir zur Abkürzung durch Θ das Jacobi'sche Symbol

(58)
$$\Theta = \left(\frac{2}{\prod_{i=1}^{\frac{n}{2}}(4a_i\mathfrak{a}_i - \mathfrak{A}_i^2)}\right)$$

bezeichnen und letzteres ergiebt sich mittels der aus (40) vorigen Capitels folgenden Congruenz

$$A \equiv \prod_{i=1}^{\frac{n}{2}} (4a_i\mathfrak{a}_i - \mathfrak{A}_i^2) \pmod{8}$$

als identisch mit

(58a)
$$\Theta = \left(\frac{2}{A}\right).$$

Daraus folgt die Anzahl der Wurzeln der Congruenz (57) für ein **gerades** α gleich

(59a)
$$2^{n-1}\left(1+\frac{\Theta}{2^{\frac{n}{2}}}\right)$$

und auf ähnliche Weise für ein **ungerades** α gleich

(59b)
$$2^{n-1}\left(1-\frac{\Theta}{2^{\frac{n}{2}}}\right).$$

Da nun aus jeder Wurzel der Congruenz (57) je 2^n Wurzeln der Congruenz (55) oder (54) hervorgehen, lässt sich hiernach auch die Anzahl der Wurzeln der letzteren für jeden Werth von α bestimmen. Insbesondere erhält man für ein **ungerades** α nach der gemachten Vorbemerkung folgendes Resultat:

Die Anzahl derjenigen Wurzeln der Congruenz (54), für welche nicht alle Zahlen (12) gerade sind, beträgt

$$2^{2n-1}\cdot\left(1-\frac{\Theta}{2^{\frac{n}{2}}}\right)$$

und demnach ist die in nr. 1, 3) unter A verstandene Zahl

(60)
$$\mathsf{A} = 2^{n-1}\left(1-\frac{\Theta}{2^{\frac{n}{2}}}\right).$$

Aus (58a) ist zu ersehen, dass diese Zahl nur von der Ordnung der Form $f(x_\varrho)$ abhängig ist. —

6. In nr. 3 sind die gesuchten Wurzelanzahlen auf einem scheinbaren Umwege bestimmt worden, insofern zuerst gewisse linear aus denselben zusammengesetzte Ausdrücke ermittelt wurden, welche dann leicht jene Anzahlen finden liessen.

Wir können aber überhaupt für unser Vorhaben, wie Minkowski durchgeführt hat, den Zahlen, die wir durch das Symbol $f\{\alpha, N\}$ ausgedrückt haben, andere Ausdrücke substituiren, die eben auf dieselbe Weise linear aus jenen gebildet sind. Setzt man nämlich

$$(61) \qquad f(h, N) = \sum_{s=1}^{N} e^{\frac{2sh\pi i}{N}} \cdot f\{s, N\},$$

so ist nicht nur die Funktion $f(h, N)$ durch die Zahlen

$$f\{\alpha, N\},$$

sondern auch umgekehrt diese durch jene bestimmt, da aus der vorigen Gleichung unmittelbar folgende hervorgeht:

$$N \cdot f\{\alpha, N\} = \sum_{h=1}^{N} e^{-\frac{2h\alpha\pi i}{N}} \cdot f(h, N).$$

Die so eingeführte Funktion $f(h, N)$ ist nichts anderes, als eine Verallgemeinerung der bekannten Gauss'schen Summe

$$\sum_{s=1}^{N} e^{\frac{2s^2h\pi i}{N}}.$$

In der That, da die Form $f(x_\varrho)$, wenn man die n Variabeln x_ϱ alle verschiedenen Reste (mod. N) durchlaufen lässt, genau $f\{s, N\}$ mal den Rest s giebt, wird in der n-fachen Summe

$$\sum e^{\frac{2h\pi i}{N} \cdot f(x_\varrho)},$$

wenn sie bezüglich jeder Variabeln x_ϱ auf ein übrigens ganz beliebiges Restsystem (mod. N) erstreckt wird, ebenfalls $f\{s, N\}$ mal der Summande $e^{\frac{2hs\pi i}{N}}$ auftreten, also die Gleichheit

$$(61\text{a}) \qquad f(h, N) = \sum e^{\frac{2h\pi i}{N} \cdot f(x_\varrho)}$$

statthaben, die Funktion $f(h, N)$ mithin als eine n-fache Gauss'sche Summe sich darstellen. H. Weber hat diesen mehrfachen Gauss'schen Summen eine schöne Arbeit gewidmet*) und gezeigt, dass sie ganz analoge Eigenschaften haben, wie die einfachen, und zu entsprechenden Sätzen, zum Theil von grosser Einfachheit, führen. Wir halten es für angezeigt, die hauptsächlichsten Resultate dieser Untersuchung unserm Werke einzufügen, werden uns aber bei ihrer Herleitung nach dem Vorgange von Minkowski die grosse Vereinfachung zu Nutze machen, welche aus der Verwendung eines Hauptrestes statt der Form $f(x_\varrho)$ entspringt.

Wir heben zunächst einige fundamentale Eigenschaften der Summe $f(h, N)$ hervor.

1) darf h prim gegen N gedacht werden. Denn, wäre im Gegentheil $h = h'd$, $N = N'd$, unter d den grössten gemeinsamen Theiler von h und N verstanden, sodass nun h', N' relativ prim sind, so wäre

$$f(h, N) = \sum e^{\frac{2h'\pi i}{N'} \cdot f(x_\varrho)},$$

wo jede Variable x_ϱ noch ein vollständiges Restsystem (mod. N) z. B. die Zahlen $1, 2, 3, \cdots N$ zu durchlaufen hat. Da aber zwei (mod. N') congruente dieser Zahlen denselben Werth des allgemeinen Gliedes der Summe ergeben, so leuchtet ein, dass jenes Glied für je d Werthe einer jeden Variabeln und somit für d^n Werthsysteme der Variabeln den gleichen Werth annimmt, mit anderen Worten, es ist

$$f(h, N) = d^n \cdot \sum{}' e^{\frac{2h'\pi i}{N'} \cdot f(x_\varrho)},$$

wo nun nur noch über vollständige Restsysteme (mod. N') zu summiren ist. Man findet also schliesslich:

$$f(h, N) = \left(\frac{N}{N'}\right)^n \cdot f(h', N'). \tag{62}$$

2) Da

$$r^2 \cdot f(x_\varrho) = f(rx_\varrho)$$

ist und, wenn r prim gegen N gedacht wird, rx_ϱ gleichzeitig

*) H. Weber, über die mehrfachen Gauss'schen Summen, Journal f. d. r. u. a. Math. 74 S. 14.

mit x_ϱ ein vollständiges Restsystem (mod. N) durchläuft, so findet sich sogleich die zweite Beziehung

(63) $$f(r^2h, N) = f(h, N)$$

für jede gegen N prime Zahl r.

3) Sei $N = P \cdot Q$, wo P, Q relative Primzahlen bedeuten. Die Variable x_ϱ wird dann ein vollständiges Restsystem (mod. N) durchlaufen, wenn man in

$$x_\varrho = Pz_\varrho + Qy_\varrho$$

y_ϱ, z_ϱ vollständige Restsysteme (mod. P) resp. (mod. Q) durchlaufen lässt. Geschieht dies für alle Werthe $1, 2, \cdots n$ des Index ϱ, so wird

$$\begin{aligned} f(x_\varrho) &= f(Pz_\varrho + Qy_\varrho) \\ &= P^2 \cdot f(z_\varrho) + Q^2 \cdot f(y_\varrho) + PQ \cdot \sum_i z_i \frac{\partial f(y_\varrho)}{\partial y_i} \end{aligned}$$

d. h.

$$f(x_\varrho) \equiv P^2 \cdot f(z_\varrho) + Q^2 \cdot f(y_\varrho) \text{ (mod. } N)$$

sein. Also wird

$$f(h, N) = \sum e^{\frac{2h\pi i}{N}(P^2 f(z_\varrho) + Q^2 f(y_\varrho))}$$

d. i. gleich dem Produkte der beiden Summen

$$\sum e^{\frac{2hPi}{Q} \cdot f(z_\varrho)}, \quad \sum e^{\frac{2hQi}{P} \cdot f(y_\varrho)}$$

von denen die erste über ein vollständiges Restsystem (mod. Q), die zweite über ein solches (mod. P) zu erstrecken ist. Dies lässt sich aber folgendermassen schreiben: Es ist

(64) $$f(h, PQ) = f(Ph, Q) \cdot f(Qh, P),$$

wenn P, Q relative Primzahlen sind.

Offenbar lässt sich dieser Satz erweitern, sodass er für eine Zerlegung der Zahl N in beliebig viele relativ prime Faktoren gilt, und gestattet daher, die Bestimmung der Funktion $f(h, N)$ für ein beliebiges N auf den Fall zurückzuführen, in welchem N eine Primzahlpotenz: $N = q^t$ ist.

4) Aehnlich, wie die Summe $f(h, N)$ in dem eben betrachteten Falle in ein Produkt von Summen zerfiel, wird dasselbe der Fall sein, wenn die quadratische Form $f(x_\varrho)$ von n Veränderlichen in eine Summe $f_1(y_\varrho) + f_2(z_\varrho) + \cdots$ qua-

dratischer Formen mit getrennten Veränderlichen $y_\varrho, z_\varrho, \cdots$ zerlegt werden kann. Die n-fache Summation $f(h, N)$ zerfällt dann, da die Summation nach den Variabeln einer der Formen von derjenigen nach den Variabeln einer anderen unabhängig ist, in das Produkt der einfacheren Summen

$$\sum e^{\frac{2h\pi i}{N}\cdot f_1(y_\varrho)}, \quad \sum e^{\frac{2h\pi i}{N}\cdot f_2(z_\varrho)}, \cdots$$

d. h. es ist

$$(65) \qquad f(h, N) = f_1(h, N)\cdot f_2(h, N)\cdots$$

Auf letzterer Formel beruht im wesentlichen die Vereinfachung der Untersuchung, welche durch Substitution eines Hauptrestes statt der Form $f(x_\varrho)$ erreicht werden kann. Solche Substitution ist aber erlaubt; denn, da ein Hauptrepräsentant $f'(y_\varrho)$, weil mit $f(x_\varrho)$ äquivalent, ebenso wohl wie sein Rest (mod. N) genau für soviel Werthsysteme der Variabeln (mod. N) congruent s wird, wie $f(x_\varrho)$ selbst, so darf man auch

$$f(h, N) = \sum e^{\frac{2h\pi i}{N}\cdot f'(y_\varrho)}$$

und nun statt $f'(y_\varrho)$ seinen Rest (mod. N) setzen.

7. Betrachten wir nun zuerst den Fall $N = p^t$, wo p eine ungerade Primzahl ist.

Diese werde erstens als eine solche vorausgesetzt, welche nicht in der Determinante A der Form $f(x_\varrho)$ aufgeht. Dann darf man nach (25) vorigen Capitels

$$f'(y_\varrho) \equiv a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2 \pmod{p^t}$$

setzen, woraus

$$(66) \qquad A \equiv a_1 a_2 \cdots a_n \pmod{p^t}$$

folgt, und man erhält nach (65) sogleich die Beziehung:

$$f(h, p^t) = \prod_{\varkappa=1}^{n} \left(\sum e^{\frac{2h a_\varkappa \pi i}{p^t}\cdot y_\varkappa^2}\right),$$

wo in jeder der n Summen über ein vollständiges Restsystem (mod. p^t) zu summiren ist. Da h zum Modulus p^t prim gedacht werden darf, wie es auch $a_\varkappa$ ist, findet sich nach der Theorie der einfachen Gauss'schen Summen*)

*) S. Analytische Zahlentheorie S. 165.

$$\sum e^{\frac{2ha_x\pi i}{p^t}\cdot y_x^2} = \left(\frac{ha_x}{p^t}\right)\cdot p^{\frac{t}{2}}\cdot i^{\left(\frac{p^t-1}{2}\right)^2}$$

und folglich zunächst

$$(67)\qquad f(h,p^t) = \left(\frac{h}{p^t}\right)^n\cdot\left(\frac{A}{p^t}\right)\cdot p^{\frac{nt}{2}}\cdot i^{n\cdot\left(\frac{p^t-1}{2}\right)^2}.$$

Ist also N, in Primzahlpotenzen zerlegt,

$$N = p^t\cdot p'^{t'}\cdot p''^{t''}\cdots,$$

so gewinnt man hieraus mit Hilfe des Satzes (64)

$$f(h,N) = \prod_p f\left(\frac{N}{p^t}h, p^t\right)$$

also gleich

$$N^{\frac{n}{2}}\left(\frac{A}{N}\right)\cdot i^{n\sum_p\left(\frac{p^t-1}{2}\right)^2}\cdot\prod_p\left(\frac{\frac{N}{p^t}h}{p^t}\right)^n.$$

Nun ist das hier auftretende Produkt gleich $\left(\frac{h}{N}\right)^n$ mal dem über jede Combination zweier Primzahlen $p, p', p'', \cdots$ erstreckten Produkte

$$\prod\left(\frac{p'^{t'}}{p^t}\right)^n\cdot\left(\frac{p^t}{p'^{t'}}\right)^n = (-1)^{n\cdot\sum\frac{p^t-1}{2}\cdot\frac{p'^{t'}-1}{2}},$$

wodurch der vorige Ausdruck mit Rücksicht auf die Beziehung

$$\sum\left(\frac{p^t-1}{2}\right)^2 + 2\sum\frac{p^t-1}{2}\cdot\frac{p'^{t'}-1}{2} = \left(\sum\frac{p^t-1}{2}\right)^2 \equiv \left(\frac{N-1}{2}\right)^2 \pmod{4}$$

in den einfacheren:

$$N^{\frac{n}{2}}\cdot\left(\frac{A}{N}\right)\cdot\left(\frac{h}{N}\right)^n\cdot i^{n\left(\frac{N-1}{2}\right)^2}$$

übergeht und sich folgende allgemeine, für jeden ungeraden und zu A primen Modulus N giltige Formel:

$$(68)\qquad f(h,N) = \left(\frac{h}{N}\right)^n\left(\frac{A}{N}\right)\cdot N^{\frac{n}{2}}\cdot i^{n\left(\frac{N-1}{2}\right)^2}$$

ergiebt, insbesondere also für $h = 1$:

$$f(1,N) = \left(\frac{A}{N}\right)\cdot N^{\frac{n}{2}}\cdot i^{n\left(\frac{N-1}{2}\right)^2},$$

das vollständige Analogon zu der für die einfachen Gauss'schen Summen und ein zu a primes, ungerades N geltenden Formel

$$\sum_{y=1}^{N} e^{\frac{2\pi i a y^2}{N}} = \left(\frac{a}{N}\right) \cdot N^{\frac{1}{2}} \cdot i^{\left(\frac{N-1}{2}\right)^2}.$$

Man sieht nun leicht, wie auf den eben betrachteten Fall der andere zurückkommt, wo p eine in der Determinante A aufgehende Primzahl ist. Denn, wenn dann o_m die erste durch p theilbare der Invarianten $o_1, o_2, \cdots o_{n-1}$ ist, mithin ω_m die erste von Null verschiedene der Zahlen $\omega_1, \omega_2, \cdots \omega_{n-1}$, so nimmt die Congruenz (25) vorigen Capitels folgende Gestalt an:

$$f'(y_\varrho) \equiv f_1(y_\varrho) + p^{\omega_m} \cdot f_2(z_\varrho) \pmod{p^t},$$

wo

$$f_1(y_\varrho) = a_1 y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2,$$

$f_2(z_\varrho)$ aber eine quadratische Form von $n-m$ anderen Variabeln ist. Hieraus erhält man aber nach (65)

$$f(h, p^t) = \sum e^{\frac{2\pi h i}{p^t}(a_1 y_1^2 + \cdots + a_m y_m^2)} \cdot \sum e^{\frac{2\pi h i}{p^{t-\omega_m}} \cdot f_2(z_\varrho)},$$

wo der erste Faktor, in Analogie mit (67), gleich

$$p^{\frac{mt}{2}} \cdot \left(\frac{h}{p^t}\right)^m \cdot \left(\frac{a_1 a_2 \cdots a_m}{p^t}\right) \cdot i^{m\left(\frac{p^t-1}{2}\right)^2},$$

der zweite aber, wenn man die z_ϱ nur noch Restsysteme (mod. $p^{t-\omega_m}$) durchlaufen lässt, gleich

$$p^{(n-m)\omega_m} \cdot f_2(h, p^{t-\omega_m})$$

gesetzt werden kann, während nun der Ausdruck

$$f_2(h, p^{t-\omega_m})$$

auf ähnliche Weise weiter reducirt werden kann u. s. f. Man erkennt aus dieser Betrachtung leicht wieder, dass allgemein $f(h, p^t)$ ausser durch die Ordnung nur durch die auf die Primzahl p bezüglichen Einzelcharaktere der Form $f(x_\varrho)$ bestimmt wird.

8. Wir wenden uns jetzt zu dem Falle, in welchem der Modulus $N = 2^t$ ist, beschränken uns jedoch dabei wieder auf die Annahme, dass die Determinante der

Form ungerade sei. Es sind in diesem Falle ungerade und gerade Formen gesondert zu behandeln.

Sei zuerst $f(x_\varrho)$ eine ungerade Form. Indem man sie in der Summe $f(h, 2^t)$ durch ihren Hauptrest ersetzt, wird

$$f(h, 2^t) = \sum e^{\frac{2\pi h i}{2^t}(a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2)},$$

wofür sich sogleich schreiben lässt

$$f(h, 2^t) = \prod_{\varkappa=1}^{n} \left(\sum e^{\frac{2\pi h i a_\varkappa}{2^t} y_\varkappa^2} \right);$$

h darf ungerade vorausgesetzt werden. Die Theorie der einfachen Gauss'schen Summen giebt nun (s. analyt. Zahlentheorie S. 153) für die Summe, welche den allgemeinen Faktor des vorstehenden Produkts bildet, jenachdem t gerade oder $t > 1$ ungerade ist, den Werth

$$2^{\frac{t}{2}}(1 + i^{h a_\varkappa}) \text{ resp. } 2^{\frac{t+1}{2}} \cdot e^{\frac{h a_\varkappa \pi i}{4}},$$

woraus, wie leicht zu bestätigen, sich allgemein für $t > 1$

$$\sum e^{\frac{2 h \pi a_\varkappa i}{2^t} y_\varkappa^2} = \left(\frac{2}{h a_\varkappa}\right)^t \cdot \left(1 + i(-1)^{\frac{h a_\varkappa - 1}{2}}\right) \cdot 2^{\frac{t}{2}}$$

ergiebt. Da zudem für $t \gtreqless 3$

$$a_1 a_2 \cdots a_n \equiv A \pmod{8},$$

wird dann

$$(69) \quad f(h, 2^t) = \left(\frac{2}{h}\right)^{nt} \cdot \left(\frac{2}{A}\right)^t \cdot 2^{\frac{nt}{2}} \cdot \prod_{\varkappa=1}^{n} \left(1 + i(-1)^{\frac{h a_\varkappa - 1}{2}}\right).$$

Nennt man nun wieder μ, ν die Anzahl der Zahlen

$$a_1, a_2, \cdots a_n,$$

welche resp. die Form $4j + 1$ oder $4j + 3$ haben, so findet man

$$\prod_{\varkappa=1}^{n} \left(1 + i(-1)^{\frac{h a_\varkappa - 1}{2}}\right) = i^\nu \cdot (-1)^{\nu \cdot \frac{h+1}{2}} \cdot \left(1 + i(-1)^{\frac{h-1}{2}}\right)^n.$$

Da $(-1)^\nu = (-1)^{\frac{A-1}{2}}$ und, wenn man $\nu = 2\left[\frac{\nu}{2}\right] + \lambda$ setzt,

$$i^\nu = (-1)^{\left[\frac{\nu}{2}\right]} \cdot i^\lambda = (-1)^{\left[\frac{\nu}{2}\right]} \cdot i^{\nu^2}$$

das vollständige Analogon zu
Summen und ein zu a pri

$$\sum_{y=1}^{N} e^{\frac{2\pi i a y^2}{N}} =$$

Man sieht nun leicht,
der andere zurückkommt
aufgehende Primzahl ist.
p theilbare der Invariant
erste von Null verschied
nimmt die Congruenz (2
an:

$$f'(y_\varrho) = f_1(y$$

wo

$$f_1(y_\varrho) = a_1 y$$

$f_2(z_\varrho)$ aber eine quadr
Variabeln ist. Hieraus

$$f(h, p^t) = \sum e^{\frac{2\pi h}{p^t}} \quad = \prod \left(\sum \right.$$

wo der erste Faktor, in ... Summe. In dem allgemeinen Fall

$$p^{\frac{mt}{2}} \cdot \left(\frac{h}{p^t}\right)^m \cdot$$

der zweite aber, wenn
(mod. p^t ...) durchlaufen ... Methode bestimmen

$$p^{(n-m)}$$

gesetzt werden kann, währ

$$f_2($$

auf ähnliche Weise weiter
erkennt aus dieser Betr
allgemein $f(h, p^t)$ ausser
die auf die Primzahl p b
der Form $f(x_\varrho)$ bestimmt

8. Wir wenden uns je
der Modulus $N = 2^t$ ist,
wieder auf die Annahme,

rtgelassen werden darf. Man
r folgenden vierfachen Summe:

$$'v' + 2\mathfrak{a}_\varkappa v'^2)$$

$$\frac{\pi h i}{-1}(2a_\varkappa u u' + \mathfrak{A}_\varkappa(u v' + u' v) + 2\mathfrak{a}_\varkappa v v')\Big),$$

genommene, als Produkt zweier

$$\sum_v e^{\frac{2h\pi i}{2^\tau - 1} v(\mathfrak{A}_\varkappa u' + 2\mathfrak{a}_\varkappa v')}$$

nun nicht gleichzeitig

$$+ 2\mathfrak{a}_\varkappa v' \equiv 0 \pmod{2^{\tau-1}}$$

$$(4a_\varkappa \mathfrak{a}_\varkappa - \mathfrak{A}_\varkappa^2)v' \equiv 0$$

$$\pmod{2^{\tau-1}},$$

ıer dieser Faktoren und damit
l der Summe (72). Es bleiben
lerselben bestehen, in welchen

$$v' = 2^{\tau-1} \cdot v_1$$

irt sich, da für letztere Werthe
toren den Werth 2^τ erhält, ein-

$$_1^2 + 2\mathfrak{A}_\varkappa u_1 v_1 + 2\mathfrak{a}_\varkappa v_1^2)$$

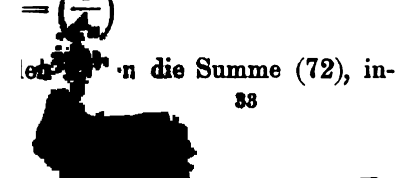
,

lige Restsysteme (mod. 2ϱ) zu
ttelbare Berechnung zeigt, dass,
den Werth $2 \cdot (-1)^{\mathfrak{a}_\varkappa}$, wenn
Jenachdem nun $\mathfrak{a}_\varkappa$ gerade oder

$$\equiv 7 \text{ oder } 3 \pmod{8}$$

$$= \left(\frac{2}{\cdot}\right)$$

le... ·n die Summe (72), in-



ist, ferner aber aus der Congruenz

$$\nu \equiv \frac{A-1}{2} \pmod{2}$$

sich

$$\nu^2 \equiv \left(\frac{A-1}{2}\right)^2 \pmod{4}$$

ergiebt, so wird

$$(70)\qquad \prod_{\varkappa}\left(1 + i(-1)^{\frac{h a_\varkappa - 1}{2}}\right)$$

$$= (-1)^{\frac{A-1}{2}\cdot\frac{h+1}{2}} \cdot (-1)^{\left[\frac{\nu}{2}\right]} \cdot i^{\left(\frac{A-1}{2}\right)^2} \cdot \left(1 + i(-1)^{\frac{h-1}{2}}\right)^n,$$

und man sieht hieraus wieder (nr. 3 u. 4), dass $f(h, 2^t)$ ausser durch die Ordnung der Form $f(x_\varrho)$ allein mittels ihres Simultancharakters $\psi(o, n-1)$ bestimmt ist.

Ist zweitens $f(x_\varrho)$ eine gerade Form, also n gerade, so findet man für $f(h, 2^t)$ folgenden Produktausdruck

$$(71)\qquad f(h, 2^t) = \prod_{\varkappa=1}^{\frac{n}{2}}\left(\sum e^{\frac{2h\pi i}{2^t}(2a_\varkappa y^2 + 2\mathfrak{A}_\varkappa yz + 2\mathfrak{a}_\varkappa z^2)}\right),$$

in welchem die Summe, die den allgemeinen Faktor bildet, bezüglich der Zahlen y, z über vollständige Restsysteme (mod. 2^t) zu erstrecken ist; h darf wieder ungerade vorausgesetzt werden. Man kann diese Summe, wie es H. Weber gethan hat, mittels derselben Methode bestimmen, welche Gauss in dem entsprechenden Falle der einfachen Gauss'schen Summen angewendet. Setzt man nämlich $2^t = 2^{2\tau}\cdot\varrho$, wo $\varrho = 1$ oder 2, jenachdem t gerade oder ungerade ist, und

$$y = 2^\tau\varrho\cdot u + u',\quad z = 2^\tau\varrho\cdot v + v',$$

so durchlaufen y, z vollständige Restsysteme (mod. 2^t), wenn u, v die kleinsten positiven Reste (mod. 2^τ) und u', v' solche (mod. $2^\tau\varrho$) durchlaufen. Der Exponent in der Summe aber nimmt die Gestalt an:

$$\frac{2\pi h i}{2^t}(2a_\varkappa u'^2 + 2\mathfrak{A}_\varkappa u'v' + 2\mathfrak{a}_\varkappa v'^2)$$

$$+ \frac{2\pi h i}{2^{\tau-1}}(2a_\varkappa uu' + \mathfrak{A}_\varkappa(uv' + u'v) + 2\mathfrak{a}_\varkappa vv')$$

$$+ 2\pi h\varrho i(2a_\varkappa u^2 + 2\mathfrak{A}_\varkappa uv + 2\mathfrak{a}_\varkappa v^2),$$

wo der letzte Bestandtheil fortgelassen werden darf. Man findet daher die Summe gleich der folgenden vierfachen Summe:

$$(72)\quad \begin{cases} \sum\limits_{u',\,v'}\Big(e^{\frac{2h\pi i}{2^t}(2a_\varkappa u'^2+2\mathfrak{A}_\varkappa u'v'+2\mathfrak{a}_\varkappa v'^2)} \\ \qquad\qquad \cdot\sum\limits_{u,\,v} e^{\frac{2\pi h i}{2^{\tau-1}}(2a_\varkappa uu'+\mathfrak{A}_\varkappa(uv'+u'v)+2\mathfrak{a}_\varkappa vv')}\Big), \end{cases}$$

in welcher die innere, nach u, v genommene, als Produkt zweier einfachen:

$$\sum_u e^{\frac{2h\pi i}{2^{\tau-1}}u(2a_\varkappa u'+\mathfrak{A}_\varkappa v')}\cdot\sum_v e^{\frac{2h\pi i}{2^{\tau-1}}v(\mathfrak{A}_\varkappa u'+2\mathfrak{a}_\varkappa v')}$$

geschrieben werden kann. Ist nun nicht gleichzeitig

$$2a_\varkappa u'+\mathfrak{A}_\varkappa v'\equiv 0,\ \mathfrak{A}_\varkappa u'+2\mathfrak{a}_\varkappa v'\equiv 0\ (\text{mod. } 2^{\tau-1})$$

d. h.

$$(4a_\varkappa\mathfrak{a}_\varkappa-\mathfrak{A}_\varkappa^2)u'\equiv 0,\ (4a_\varkappa\mathfrak{a}_\varkappa-\mathfrak{A}_\varkappa^2)v'\equiv 0$$

und folglich

$$u'\equiv v'\equiv 0\ (\text{mod. } 2^{\tau-1}),$$

so verschwindet wenigstens einer dieser Faktoren und damit zugleich das entsprechende Glied der Summe (72). Es bleiben sonach nur diejenigen Glieder derselben bestehen, in welchen

$$u'=2^{\tau-1}\cdot u_1,\ v'=2^{\tau-1}\cdot v_1$$

ist, und die ganze Summe reducirt sich, da für letztere Werthe von u', v' jeder der vorigen Faktoren den Werth 2^τ erhält, einfach auf die folgende:

$$2^{2\tau}\cdot\sum e^{\frac{2h\pi i}{4\varrho}(2a_\varkappa u_1^2+2\mathfrak{A}_\varkappa u_1v_1+2\mathfrak{a}_\varkappa v_1^2)},$$

in welcher nun u_1, v_1 vollständige Restsysteme (mod. 2ϱ) zu durchlaufen haben. Eine unmittelbare Berechnung zeigt, dass, wenn $\varrho=1$ ist, die Summe den Werth $2\cdot(-1)^{\mathfrak{a}_\varkappa}$, wenn $\varrho=2$ ist, den Werth 4 hat. Jenachdem nun $\mathfrak{a}_\varkappa$ gerade oder ungerade ist, wird

$$A_\varkappa=4a_\varkappa\mathfrak{a}_\varkappa-\mathfrak{A}_\varkappa^2\equiv 7 \text{ oder } 3\ (\text{mod. } 8)$$

also stets

$$(-1)^{\mathfrak{a}_\varkappa}=\left(\frac{2}{A_\varkappa}\right)$$

sein. Man darf demnach in allen Fällen die Summe (72), in-

dem man dies Jacobi'sche Symbol zur Abkürzung mit θ_κ bezeichnet, gleich

$$(2\theta_\kappa)^{2\tau+\varrho} = (2\theta_\kappa)^{t+1}$$

setzen und findet sodann nach (71) die Formel:

$$f(h, 2^t) = 2^{\frac{n(t+1)}{2}} \cdot \Theta^{t+1},$$

wenn unter Θ wieder das Symbol (58) verstanden wird, oder einfacher:

$$f(h, 2^t) = 2^{\frac{n(t+1)}{2}} \cdot \left(\frac{2}{A}\right)^{t+1}. \tag{73}$$

Diese Formel zeigt, dass im gegenwärtigen Falle $f(h, 2^t)$ nur von der Ordnung der Form $f(x_\varrho)$ bestimmt wird.

Kürzer kommt man zu demselben Resultat, indem man die Bestimmung der Summe (71) auf den vorigen Fall einer ungeraden Form zurückführt. Betrachtet man nämlich die ungerade Form

$$\xi^2 + 2a_\kappa y^2 + 2\mathfrak{A}_\kappa yz + 2\mathfrak{a}_\kappa z^2$$

mit der ungeraden Determinante

$$A_\kappa = 4a_\kappa\mathfrak{a}_\kappa - \mathfrak{A}_\kappa^2$$

und bildet einen ihrer Hauptreste (mod. 2^t), so wird dieser die Form haben

$$\alpha x^2 + \alpha' x'^2 + \alpha'' x''^2,$$

woraus für $t \gtrless 3$

$$\alpha\alpha'\alpha'' \equiv A_\kappa \pmod{8} \tag{74}$$

hervorgeht. In Folge davon wird

$$\sum e^{\frac{2h\pi i}{2^t}(\xi^2+2a_\kappa y^2+2\mathfrak{A}_\kappa yz+2\mathfrak{a}_\kappa z^2)} = \sum e^{\frac{2h\pi i}{2^t}(\alpha x^2+\alpha' x'^2+\alpha'' x''^2)}$$

d. i. nach (69) gleich

$$\left(\frac{2}{h}\right)^{3t} \cdot \left(\frac{2}{A_\kappa}\right)^t \cdot 2^{\frac{3t}{2}} \tag{75}$$

mal dem Produkte

$$\left(1 + i(-1)^{\frac{h\alpha-1}{2}}\right)\left(1 + i(-1)^{\frac{h\alpha'-1}{2}}\right)\left(1 + i(-1)^{\frac{h\alpha''-1}{2}}\right), \tag{75a}$$

welch letzteres nach (70) gleich

$$(-1)^{\frac{A_\kappa-1}{2}\cdot\frac{h+1}{2}} \cdot (-1)^{\left[\frac{\nu}{2}\right]} \cdot i^{\left(\frac{A_\kappa-1}{2}\right)^2} \cdot \left(1 + i(-1)^{\frac{h-1}{2}}\right)^3$$

gesetzt werden kann, wenn ν die Anzahl der Zahlen $\alpha, \alpha', \alpha''$, welche von der Form $4j+3$ sind, also, da

$$A_\varkappa = 4a_\varkappa \mathfrak{a}_\varkappa - \mathfrak{A}_\varkappa^2 \equiv -1 \pmod{4}$$

ist, 1 oder 3 bedeutet. Da nun andererseits

$$\sum e^{\frac{2h\pi i}{2^t}\xi^2} = \left(\frac{2}{h}\right)^t \cdot \left(1 + i(-1)^{\frac{h-1}{2}}\right) \cdot 2^{\frac{t}{2}}$$

ist, liefert die Division beider Summen durch einander das Ergebniss:

$$\sum e^{\frac{2h\pi i}{2^t}(2a_\varkappa y^2 + 2\mathfrak{A}_\varkappa yz + 2\mathfrak{a}_\varkappa z^2)}$$

$$= 2^t \cdot \left(\frac{2}{A_\varkappa}\right)^t \cdot \left(1 + i(-1)^{\frac{h-1}{2}}\right)^2 \cdot (-1)^{\frac{h+1}{2} \cdot \frac{A_\varkappa - 1}{2}}$$

$$\cdot i^{\left(\frac{A_\varkappa - 1}{2}\right)^2} \cdot (-1)^{\left[\frac{\nu}{2}\right]},$$

was, vereinfacht, gleich

$$2^{t+1} \cdot \left(\frac{2}{A_\varkappa}\right)^t \cdot (-1)^{\left[\frac{\nu}{2}\right]}$$

und mit dem auf dem früheren Wege Gefundenen identisch ist, wenn man zeigen kann, dass

$$(-1)^{\left[\frac{\nu}{2}\right]} = \left(\frac{2}{A_\varkappa}\right) = \theta_\varkappa$$

ist. Dies folgt aber aus der Bemerkung, dass die Congruenzen

$$\xi^2 + 2a_\varkappa y^2 + 2\mathfrak{A}_\varkappa yz + 2\mathfrak{a}_\varkappa z^2 \equiv 1 \pmod{4}$$

und

$$\alpha x^2 + \alpha' x'^2 + \alpha'' x''^2 \equiv 1 \pmod{4}$$

die gleiche Anzahl Wurzeln haben müssen; die erstere von ihnen hat, da ξ ungerade und $a_\varkappa y^2 + \mathfrak{A}_\varkappa yz + \mathfrak{a}_\varkappa z^2$ gerade sein muss, $8(2+\theta_\varkappa)$ Wurzeln, die zweite aber, jenachdem $\nu = 1$ oder 3 ist, 24 oder 8 d. i.

$$8\left(2 + (-1)^{\left[\frac{\nu}{2}\right]}\right)$$

Wurzeln, woraus in der That

$$(-1)^{\left[\frac{\nu}{2}\right]} = \theta_\varkappa.$$

Achtes Capitel.

Neue Definition des Geschlechts.

1. Im sechsten Capitel sind diejenigen Classen einer gegebenen Ordnung, welche gleiche Charaktere haben, als ein Geschlecht von Classen oder Formen definirt worden. Das Geschlecht, welchem eine gegebene Form f von n Variabeln angehört, bilden also diejenigen Formen, welche dieselbe Anzahl der Variabeln, denselben Index τ, dieselben Invarianten und dieselben quadratischen Charaktere besitzen wie f. Nun hat Minkowski an Stelle dieser Definition eine andere gesetzt, welche sich als geeigneter erweist, namentlich insofern, als sie eine tiefere Einsicht bezüglich des Maasses eines Geschlechts gewährt, von dem wir später ausführlich handeln werden. Indem wir diese entwickeln wollen, führen wir vor allem den Begriff ein, auf welchen sie sich gründet.

Wir nennen die Classen zweier Formen f und g (von n Veränderlichen und demselben Trägheitsindex τ) einander (mod. N) congruent, in Zeichen:

$$f \simeq g \pmod{N}, \tag{1}$$

wenn es in der Classe von f eine Form φ und in der Classe von g eine Form ψ giebt, welche (mod. N) denselben Rest lassen, für welche also

$$\varphi \equiv \psi \pmod{N} \tag{2}$$

ist.

Aus dieser Erklärung fliessen sogleich einige einfache Folgerungen.

1) Sind die Classen von f und g einander (mod. N) congruent, so ist jede Form der ersteren Classe einer Form der zweiten congruent. Denn, wendet man auf φ jede Substitution $(q_{i\varkappa})$ mit dem Modulus 1 an, so entsteht jede Form

$$\varphi' = (q_{\varkappa i}) \cdot \varphi \cdot (q_{i\varkappa})$$

der Classe von f, und ebenso aus ψ je eine Form

$$\psi' = (q_{\varkappa i}) \cdot \psi \cdot (q_{i\varkappa})$$

der Classe von g, wegen (2) aber ist

$$\psi' \equiv \varphi' \pmod{N}.$$

Hieraus folgt offenbar, dass die Reste der Formen der einen Classe mit den Resten der Formen der anderen, in geeigneter Reihenfolge genommen, übereinstimmen.

2) Aus $f \simeq g$ und $f \simeq g' \pmod{N}$ folgt auch

$$g \simeq g' \pmod{N}.$$

Denn, da nach der letzten Bemerkung die Reste der Formen in der Classe von f sowohl mit den Resten der Formen in der Classe von g, als auch mit denjenigen der Formen in der Classe von g', in geeigneter Reihenfolge gedacht, übereinstimmen, so müssen auch die Reste der Formen in der Classe von g, mit denjenigen in der Classe von g' in geeigneter Reihenfolge genommen, es thun, mithin enthält die Classe von g' zu jeder Form ψ von g eine Form ψ', für welche

$$\psi \equiv \psi' \pmod{N}$$

ist, und es ist also

$$g \simeq g' \pmod{N}.$$

Auf Grund dieser Bemerkungen behaupten wir nun: Das Geschlecht von f wird von denjenigen Classen von Formen gebildet, welche von gleicher Variabelnanzahl und gleichem Index τ und mit der Classe von f nach jedem Modulus congruent sind. Um dies zu beweisen, haben wir zweierlei zu zeigen:

Erstens, dass jede Classe von Formen, welche n Variabeln und den Index τ hat und derjenigen von f nach jedem Modulus congruent ist, zu demselben Geschlecht gehört, wie f; und

Zweitens, dass jede Classe des Geschlechts von f mit der Classe von f nach jedem Modulus congruent ist.

Bei diesem Nachweise setzen wir, wie von nun an überhaupt, die Determinante der Formen als ungerade voraus.

Wir beginnen mit dem ersten Nachweise, welcher einfacher zu leisten ist, und fragen deshalb nach den Bedingungen, unter welchen die Classe von g (bei gleicher Variabelnzahl und gleichem Index wie f) der Classe von f nach jedem Modulus N congruent sein kann. Sei q^t eine hinreichend hohe Potenz einer Primzahl q.

Wegen der Annahme $f \simeq g$ (mod. q^t) müssen die Reste (mod. q^t) der Formen der Classe von f mit denjenigen der Classe von g in gewisser Reihenfolge übereinstimmen; ist mithin f' ein Hauptrepräsentant der ersteren Classe (mod. q^t), so giebt es eine Form g' der zweiten Classe von der Beschaffenheit, dass $f' \equiv g'$ (mod. q^t) ist. Wenn q zunächst ungerade ist, so lehrt die Congruenz (25) des sechsten Capitels bei hinreichend grossem t nicht nur für f', sondern auch für g' die entsprechenden Zahlen ω_m d. i. die höchsten in den o-Invarianten der Formen f, g aufgehenden Potenzen von q kennen und zeigt, dass dieselben für die Form g mit denjenigen für die Form f übereinstimmen müssen. Ist aber $q = 2$, so schliesst man in gleicher Weise aus der Congruenz (47) daselbst nicht nur, dass die höchsten Potenzen von 2, welche in den o-Invarianten beider Formen enthalten sind, die gleichen, sondern auch, dass die σ-Invarianten beider Formen übereinstimmen. Soll mithin $f \simeq g$ sein nach jedem beliebigen Modulus, so ersieht man sogleich, dass die o-Invarianten, wie die σ-Invarianten für beide Formen dieselben d. h. dass die beiden Formen von gleicher Ordnung sein müssen. — Also haben sie auch gleiche Determinante Δ; und da nun nach der Voraussetzung $f \simeq g$ (mod. 2Δ) sein soll, so wird, wenn jetzt f' irgend eine (mod. 2Δ) charakteristische Form der Classe von f bezeichnet, in der Classe von g eine Form g' vorhanden sein müssen, für welche

$$f' \equiv g' \pmod{2\Delta} \tag{3}$$

ist. Diese Form ist jedenfalls ein Hauptrepräsentant der Classe von g (mod. 2Δ), man darf sie aber, wie aus nr. 9 des sechsten Capitels hervorgeht, auch als eine charakteristische Form dieser Classe voraussetzen, und demnach erschliesst man dann mittels der Congruenzen

$$\sigma_m d_{m-1} f'_m \equiv \sigma_m d_{m-1} g'_m \pmod{q^{t+\partial_m-2}}$$

resp.

$$\sigma_m d_{m-1} f'_m \equiv \sigma_m d_{m-1} g'_m \pmod{\sigma_{m-1} 2^{t_0+\partial_m-2}},$$

welche für die einzelnen in 2Δ enthaltenen Primzahlpotenzen aus (3) hervorgehen, wie man unschwer erkennt, den Umstand, dass f'_m und g'_m bezüglich jedes der in Frage kommen-

den Moduln gleiche quadratische Charaktere haben müssen.

Aus alle diesem hat man zu schliessen: dass, wenn die Classe von g nach jedem Modulus der Classe von f congruent sein soll, sie nothwendigerweise gleiche Ordnung und gleiche Charaktere haben, also zu demselben Geschlechte gehören muss, wie f.

2. Indem wir uns nun zu dem schwierigeren Theile unserer Aufgabe, dem Nachweise des umgekehrten Satzes, wenden, beginnen wir mit einer Vorbemerkung. Im vorigen Capitel ist festgestellt, dass für eine Form $f(x_\varrho)$ der Ausdruck $f(h, p^t)$ und — da die Determinante der Form ungerade vorausgesetzt ist — auch der Ausdruck $f(h, 2^{t_0})$ durch das Geschlecht der Form vollständig bestimmt wird.

Ist demnach $g(x_\varrho)$ eine Form aus demselben Geschlechte wie f, so werden nicht nur, auf jede Primzahl bezüglich, die Gleichungen

$$(4) \qquad \omega_m(f) = \omega_m(g)$$

$$(5) \qquad \sigma_m(f) = \sigma_m(g)$$

$$(m = 1, 2, \cdots n - 1),$$

sondern auch die folgenden beiden erfüllt sein:

$$(6a) \qquad f(h, p^t) = g(h, p^t)$$

$$(6b) \qquad f(h, 2^{t_0}) = g(h, 2^{t_0}).$$

Da ausserdem die Determinante beider Formen f, g — nennen wir sie $\Delta(f)$, $\Delta(g)$ — einander gleich, also auch nach jedem Modulus congruent sind, hat man die Congruenz

$$(7a) \qquad \Delta(f) \equiv \Delta(g) \pmod{p^{t+\partial_{n-2}}}$$

resp.

$$(7b) \qquad \Delta(f) \equiv \Delta(g) \pmod{\sigma_{n-1}\, 2^{t_0+\partial_{n-2}}},$$

in welchen ∂_{n-2} die auf die Primzahl p resp. 2 bezügliche Zahl $\partial_{n-2}(f) = \partial_{n-2}(g)$ ist.

Lässt sich demnach zeigen, dass die Classen zweier Formen f, g, welche den Bedingungen (4) bis (7) Genüge leisten, nach dem Modulus p^t resp. 2^{t_0} einander congruent sind, so wird dies auch gelten von den Classen zweier Formen f, g, welche gleichen Geschlechts sind, und letztere folglich nach jedem

Primzahlpotenz-Modulus, also auch — wie aus nr. 7 des sechsten Capitels zu erkennen ist — für jeden beliebigen Modulus überhaupt congruent sein. Es wird sogar genügen, den gedachten Umstand für solche Primzahlpotenzen nachzuweisen, die eine gewisse Grenze überschreiten, da Classen, welche nach einem bestimmten Modulus congruent sind, es auch nach jedem Theiler desselben sein müssen; und so dürfen wir $t > v_{n-1}$ und $t_0 > 1 + v_{n-1}$ voraussetzen. Wir betrachten nur primitive Formen.

Es handle sich nun zuerst um einen Modulus p^t. Setzen wir also voraus, für die (gegen p primen) Formen f, g bestände ausser den, der Primzahl p entsprechenden Gleichungen (4) die Beziehung

$$f(h, p^t) = g(h, p^t) \quad (t > v_{n-1}), \tag{6a}$$

sowie die Congruenz (7a):

$$\Delta(f) \equiv \Delta(g) \pmod{p^{t+\partial_n - 2}}.$$

Da $f(x_\varrho), g(x_\varrho)$ prim gegen p sind, lässt die Congruenz

$$f(x_\varrho) \equiv \alpha \pmod{p^t}$$

wie die Congruenz

$$g(x_\varrho) \equiv \alpha \pmod{p^t}$$

für ein- und dasselbe durch p nicht theilbare α eine Lösung zu. Seien $x_1, x_2, \cdots x_n$ eine solche Lösung der ersteren dieser Congruenzen. Da diese Zahlen nicht sämmtlich durch p theilbar sein können, giebt es Zahlen

$$\xi_1 \equiv x_1,\ \xi_2 \equiv x_2, \cdots \xi_n \equiv x_n \pmod{p^t}$$

welche ohne gemeinsamen Theiler sind, und eine unimodulare Substitution

$$\begin{pmatrix} \xi_1 & \cdot & \cdot & \cdot & \cdot \\ \xi_2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \xi_n & \cdot & \cdot & \cdot & \cdot \end{pmatrix},$$

in welcher dieselben die erste Spalte bilden und durch welche sich die Form $f(x_\varrho)$ in eine äquivalente Form φ verwandelt, deren erster Coefficient $f(\xi_\varrho) \equiv \alpha \pmod{p^t}$ ist; die Form φ aber geht, gerade wie bei Herleitung der Formel (22) des sechsten Capitels, durch eine geeignete weitere Substitution,

welche die erste Spalte nicht verändert, in eine äquivalente Form ψ über, welche der Congruenz

$$\psi \equiv \alpha\xi^2 + p^{\omega_1} \cdot f'(x_\varrho') \pmod{p^t}$$

genügt, unter $f'(x_\varrho')$ eine Form von $n-1$ Veränderlichen verstanden, für welche die Beziehung besteht:

$$\omega_{m-1}(f') = \omega_m(f), \tag{8}$$
$$(m = 2, 3, \cdots n-1)$$

und zudem ergiebt sich nach Formel (65) und (62) vorigen Capitels diese andere, in welcher $t' = t - \omega_1$ ist:

$$\psi(h, p^t) = \sum e^{\frac{2h\alpha\pi i}{p^t}\xi^2} \cdot p^{(n-1)\omega_1} \cdot f'(h, p^{t'}), \tag{9}$$

auch schliesst man noch aus der für ψ bestehenden Congruenz (mod. p^t) die folgende:

$$\Delta(f') \cdot p^{(n-1)\omega_1} \equiv \frac{\Delta(f)}{\alpha} \pmod{p^{t+\partial_{n-2}}}. \tag{10}$$

Aus ganz gleichen Erwägungen aber gelangt man zu dem Ergebniss, dass auch die Form $g(x_\varrho)$ einer Form χ äquivalent ist, für welche

$$\chi \equiv \alpha\xi^2 + p^{\omega_1} \cdot g'(x_\varrho') \pmod{p^t}$$

ist und die Beziehungen

$$\omega_{m-1}(g') = \omega_m(g) \tag{11}$$
$$(m = 2, 3, \cdots n-1)$$

$$\chi(h, p^t) = \sum e^{\frac{2h\alpha\pi i}{p^t}\cdot\xi^2} \cdot p^{(n-1)\omega_1} \cdot g'(h, p^{t'}) \tag{12}$$

und die Congruenz

$$\Delta(g') \cdot p^{(n-1)\omega_1} \equiv \frac{\Delta(g)}{\alpha} \pmod{p^{t+\partial_{n-2}}} \tag{13}$$

erfüllt sind. Da nun wegen (6a)

$$\psi(h, p^t) = \chi(h, p^t)$$

sein muss, findet sich aus (9) und (12) die Gleichung

$$f'(h, p^{t'}) = g'(h, p^{t'}) \tag{14}$$

während aus (4), (8) und (11)

$$\omega_{m-1}(f') = \omega_{m-1}(g') \tag{15}$$
$$(m = 2, 3, \cdots n-1)$$

und (für $n > 2$) aus (10) und (13)

$$\Delta(f') \equiv \Delta(g') \pmod{p^{t'+\partial'_{n-3}}} \quad (t' > v'_{n-2}) \tag{16}$$

hervorgeht. Die Beziehungen (14) bis (16) sind aber für die Formen f', g' mit $n-1$ Veränderlichen, welche, wie f und g, prim gegen p sind, dasselbe, wie die Bedingungen (4) bis (7) für die Formen f, g mit n Veränderlichen. Setzt man daher die Richtigkeit unseres Satzes für Formen von $n-1 \gtreqless 2$ Veränderlichen voraus, so ergiebt sich die Folgerung: Wenn die Voraussetzungen (4), (6) und (7) (mod. p^t), $(t > v_{n-1})$ erfüllt sind, so sind die Classen der beiden Formen

$$f',\, g' \text{ (mod. } p^{t'}) \;\; (t' > v'_{n-2})$$

congruent d. h. durch eine geeignete, nur die Veränderlichen von f' betreffende Substitution geht f' in eine äquivalente Form $f''(x'_\varrho)$ über, welche mit $g'(x'_\varrho)$ (mod. $p^{t'}$) congruent ist, und somit zugleich ψ in eine andere äquivalente Form ψ', welche der Congruenz

$$\psi' \equiv \alpha\xi^2 + p^{\omega_1} \cdot f''(x'_\varrho) \equiv \chi \text{ (mod. } p^t)$$

genügt, man erhält mit anderen Worten

$$f \simeq g \text{ (mod. } p^t).$$

Auf solche Weise wird unsere Behauptung bezüglich des Modulus p^t für zwei Formen mit n Veränderlichen bewiesen sein, wenn man nachweisen kann, dass sie für zwei Formen von zwei Veränderlichen erfüllt ist. Dies ist aber leicht zu bestätigen, denn, versteht man im Vorigen unter f, g zwei solche Formen, so nehmen die Congruenzen für ψ und χ die Gestalt an:

$$\psi \equiv \alpha\xi^2 + p^{\omega_1}\beta x'^2,\; \chi \equiv \alpha\xi^2 + p^{\omega_1}\gamma x'^2 \text{ (mod. } p^t),$$

wo wegen (10) und (13)

$$p^{\omega_1}\beta \equiv p^{\omega_1}\gamma \text{ (mod. } p^t)$$

also auch

$$\psi \equiv \chi \text{ (mod. } p^t)$$

gefunden wird.

3. Wir betrachten zweitens den Modulus 2^{t_0},

$$t_0 > v_{n-1} + 1.$$

Seien also f, g zwei (gegen 2 prime) Formen, für welche die Beziehungen (4), (5), (7b) sowie endlich die Gleichung

$$f(h, 2^{t_0}) = g(h, 2^{t_0}) \tag{17}$$

erfüllt sind; dann ist zu zeigen, dass $f \simeq g$ (mod. 2^{t_0}). Da

dieser Umstand stattfindet, sobald er für zwei mit f resp. g äquivalente Formen erfüllt ist, und da die vorausgesetzten Beziehungen, wenn sie für f und g stattfinden, auch für zwei mit ihnen äquivalente Formen zutreffend sind, so braucht man den behaupteten Satz nur für zwei Hauptrepräsentanten f_0, g_0 der Classen von f, g (mod. 2^{t_0}) zu beweisen.

Sei zuerst $\sigma_1 = 1$. Da die Determinante ungerade gedacht wird, nehmen die vorausgesetzten Beziehungen die Gestalt an:

$$\omega_m(f) = \omega_m(g) = 0$$
$$\sigma_m(f) = \sigma_m(g) = 1$$
$$(m = 1, 2, \cdots n-1)$$

und

$$\varDelta(f) \equiv \varDelta(g) \text{ (mod. } 2^{t_0}),$$

und nach (31) des sechsten Capitels darf man

$$(18) \qquad f_0 \equiv ax_1^2 + a'x_2^2 + \cdots + a^{(n-1)}x_n^2 \text{ (mod. } 2^{t_0})$$

voraussetzen, wo $a, a', \cdots a^{(n-1)}$ ungerade Zahlen sind. Sei α irgend eine der ungeraden Zahlen, für welche die Congruenz $f_0(x_\varrho) \equiv \alpha$ (mod. 2^{t_0}) eine Lösung in nicht lauter ungeraden Zahlen $x_1, x_2, \cdots x_n$ besitzt (z. B. wäre $\alpha = a$ eine solche Zahl); da $x_1, x_2, \cdots x_n$ auch nicht sämmtlich gerade sein können, lassen sich Zahlen

$$\xi_1 \equiv x_1, \ \xi_2 \equiv x_2, \cdots \xi_n \equiv x_n \text{ (mod. } 2^{t_0})$$

so wählen, dass sie des letzteren Umstandes willen ohne gemeinsamen Theiler, des ersteren wegen nicht sämmtlich ungerade sind. Alsdann lässt sich eine unimodulare Substitution mit der ersten Vertikalreihe $\xi_1, \xi_2, \cdots \xi_n$ bilden, durch welche die Form f_0 in eine äquivalente Form mit dem ersten Coefficienten $f_0(\xi_\varrho) \equiv \alpha$ (mod. 2^{t_0}) übergeht, und diese lässt sich weiter durch eine Substitution, welche die erste Vertikalreihe nicht ändert, in eine äquivalente Form ψ verwandeln, für welche eine Congruenz stattfindet von folgender Gestalt:

$$(19) \qquad \psi \equiv \alpha\xi^2 + f'(x_\varrho') \text{ (mod. } 2^{t_0});$$

die Form $f'(x_\varrho')$ ist prim gegen 2 und es findet sich, gerade wie in nr. 4 des sechsten Capitels,

$$\omega_{m-1}(f') = \omega_m(f)$$
$$(m = 2, 3, \cdots n-1)$$



sowie, falls $\sigma_1(f') = 1$ ist, auch

$$\sigma_{m-1}(f') = \sigma_m(f)$$
$$(m = 2, 3, \cdots n-1)$$

und endlich mittels des bekannten Hilfssatzes die Congruenz

$$\Delta(f') \equiv \frac{\Delta(f)}{\alpha} \pmod{2^{t_0}}.$$

Dass aber $\sigma_1(f') = 1$ ist, davon überzeugt man sich leicht. Ist nämlich

$$(20) \qquad \begin{pmatrix} \xi_1 & \eta_1' & \cdots & \eta_1^{(n-1)} \\ \xi_2 & \eta_2' & \cdots & \eta_2^{(n-1)} \\ \cdot & \cdot & \cdot & \cdot \\ \xi_n & \eta_n' & \cdots & \eta_n^{(n-1)} \end{pmatrix}$$

die unimodulare Substitution, durch welche f_0 in ψ verwandelt wird, so ergäben sich, falls $\sigma_1(f') = 2$ wäre, aus der Congruenz (19) die Bedingungen:

$$\left.\begin{aligned} a\xi_1\eta_1^{(i)} + a'\xi_2\eta_2^{(i)} + \cdots + a^{(n-1)}\xi_n\eta_n^{(i)} &\equiv 0 \\ a\eta_1^{(i)2} + a'\eta_2^{(i)2} + \cdots + a^{(n-1)}\eta_n^{(i)2} &\equiv 0 \end{aligned}\right\} \pmod{2},$$
$$(i = 1, 2, \cdots n-1)$$

aus denen diese anderen:

$$(\xi_1 - 1)\eta_1^{(i)} + (\xi_2 - 1)\eta_2^{(i)} + \cdots + (\xi_n - 1)\eta_n^{(i)} \equiv 0$$
$$(i = 1, 2, \cdots n-1)$$

folgen; fügt man ihnen die offenbar stattfindende:

$$(\xi_1 - 1)\xi_1 + (\xi_2 - 1)\xi_2 + \cdots + (\xi_n - 1)\xi_n \equiv 0$$

hinzu, so liefern sie

$$\xi_1 - 1 \equiv \xi_2 - 1 \equiv \cdots \equiv \xi_n - 1 \equiv 0 \pmod{2}$$

entgegen den bezüglich der Zahlen $\xi_1, \xi_2, \cdots \xi_n$ getroffenen Bestimmungen.

Für die Form g_0 gelten ganz dieselben Betrachtungen. Indem wir mit β irgend eine der ungeraden Zahlen bezeichnen, für welche die Congruenz

$$g_0(x_\varrho) \equiv \beta \pmod{2^{t_0}}$$

in nicht lauter ungeraden Zahlen auflösbar ist, finden wir g_0 mit einer Form χ äquivalent, welche der Congruenz

$$(21) \qquad \chi \equiv \beta\xi^2 + g'(x_\varrho') \pmod{2^{t_0}}$$

genügt, und erhalten für die gegen 2 prime Form $g'(x_\varrho')$ die

Beziehungen

$$\omega_{m-1}(g') = \omega_m(g)$$
$$\sigma_{m-1}(g') = \sigma_m(g)$$
$$(m = 2, 3, \cdots n-1)$$

sowie die Congruenz

$$\Delta(g') \equiv \frac{\Delta(g)}{\beta} \pmod{2^{t_0}}.$$

Man darf aber $\beta = \alpha$ voraussetzen. Zum Beweise bemerke man zuvörderst, dass nach der vorausgesetzten Gleichung (17) auch

$$f\{\alpha, 2^{t_0}\} = g\{\alpha, 2^{t_0}\}$$

ist, dass also für jedes α die Congruenz

$$f_0(x_\varrho) \equiv \alpha \pmod{2^{t_0}}$$

die gleiche Anzahl Wurzeln hat, wie die Congruenz

$$g_0(x_\varrho) \equiv \alpha \pmod{2^{t_0}}.$$

Ist nun zuerst n gerade, so lässt keine der beiden Congruenzen eine Lösung in lauter ungeraden Zahlen zu, man darf folglich $\beta = \alpha$ wählen. — Ist aber $n > 1$ ungerade, so bemerke man, dass die Form $f_0(x_\varrho)$, da sie offenbar für $\frac{1}{2} \cdot 2^{n t_0}$ Restsysteme $x_1, x_2, \cdots x_n \pmod{2^{t_0}}$ ungerade wird, und unter ihnen sich $2^{n(t_0-1)}$ Restsysteme in lauter ungeraden Zahlen befinden, für $\frac{1}{2} 2^{n t_0}\left(1 - \frac{1}{2^{n-1}}\right)$ Systeme, die nicht alle ungerade sind, einen ungeraden Rest lässt. Dasselbe gilt von der Form $g_0(x_\varrho)$, zudem lässt aber letztere, wie bemerkt, jeden möglichen ihrer Reste genau so oft wie die Form $f_0(x_\varrho)$. Wenn demnach sämmtliche ungeraden Reste der Form $g_0(x_\varrho)$, welche sie für nicht lauter ungerade $x_1, x_2, \cdots x_n$ liefert, von den Resten α verschieden wären, welche so von der Form $f_0(x_\varrho)$ geliefert werden, so müssten die letzteren von der Form $g_0(x_\varrho)$ mittels lauter ungerader $x_1, x_2, \cdots x_n$ geliefert werden, und somit müsste gewiss

$$2^{n(t_0-1)} \gtreqless \frac{1}{2} 2^{n t_0}\left(1 - \frac{1}{2^{n-1}}\right)$$

sein, was nicht der Fall ist. Mithin darf man auch in diesem Falle $\beta = \alpha$ wählen.

Und sonach erschliesst man aus den für f', g' erhaltenen

Beziehungen diese anderen:

$$\omega_{m-1}(f') = \omega_{m-1}(g') = 0$$
$$\sigma_{m-1}(f') = \sigma_{m-1}(g') = 1$$
$$\Delta(f') \equiv \Delta(g') \pmod{2^{t_0}}.$$

Zu ihnen kommt endlich, ganz wie im Falle des Modulus p^t, noch die Gleichheit

$$f'(h, 2^{t_0}) = g'(h, 2^{t_0})$$

hinzu, sodass die beiden Formen f', g', da zudem $\sigma_1(f') = 1$, ganz analogen Voraussetzungen genügen, wie die ursprünglichen Formen f, g. Setzt man daher den zu beweisenden Satz für Formen mit $n-1$ Variabeln als richtig voraus, so ergiebt sich seine Richtigkeit auch für Formen mit n Variabeln; und da er für Formen mit 2 Variabeln wieder unmittelbar einleuchtet, ist er allgemeingiltig bewiesen.

4. Sei zweitens $\sigma_1 = 2$. Der ungeraden Determinante wegen kann dann

$$f_0 \equiv \sum_{i=1}^{\frac{n}{2}} 2(a_i x_{2i-1}^2 + \mathfrak{A}_i x_{2i-1} x_{2i} + \mathfrak{a}_i x_{2i}^2) \pmod{2^{t_0}}$$

vorausgesetzt werden. Ist nun α irgend eine der ungeraden Zahlen, deren Doppeltes durch die gerade Form f_0 darstellbar ist, so leuchtet ein, dass nicht sämmtliche darstellenden Zahlen $x_1, x_2, \cdots x_n$ gerade sein können, und folglich lassen sich Zahlen

$$\xi_1 \equiv x_1,\ \xi_2 \equiv x_2,\ \cdots \xi_n \equiv x_n \pmod{2^{t_0}}$$

ohne gemeinsamen Theiler, welche also auch nicht sämmtlich gerade sind, und ihnen entsprechend eine unimodulare Substitution bestimmen, deren erste Vertikalreihe jene Zahlen bilden und durch welche f_0 in eine äquivalente Form mit dem ersten Coefficienten

$$f_0(\xi_\varrho) \equiv 2\alpha \pmod{2^{t_0}}$$

übergeht. In dieser Form

$$\varphi = \sum b_{ik} y_i y_k$$

können nicht sämmtliche Coefficienten $b_{12}, b_{13}, \cdots b_{1n}$ gerade

sein; denn, ist (20) die Substitution, so wird

$$b_{1,\varkappa+1} \equiv \sum_i \left(2a_i \mathfrak{x}_{2i-1} \cdot \eta_{2i-1}^{(\varkappa)} + \mathfrak{A}_i(\mathfrak{x}_{2i-1}\eta_{2i}^{(\varkappa)} + \mathfrak{x}_{2i}\eta_{2i-1}^{(\varkappa)}) \right.$$
$$\left. + 2\mathfrak{a}_i \mathfrak{x}_{2i}\eta_{2i}^{(\varkappa)}\right) \pmod{2}$$

also

$$b_{1,\varkappa+1} \equiv \mathfrak{x}_1\eta_2^{(\varkappa)} + \mathfrak{x}_2\eta_1^{(\varkappa)} + \mathfrak{x}_3\eta_4^{(\varkappa)} + \mathfrak{x}_4\eta_3^{(\varkappa)} + \cdots$$
$$+ \mathfrak{x}_{n-1}\eta_n^{(\varkappa)} + \mathfrak{x}_n\eta_{n-1}^{(\varkappa)} \pmod{2};$$

wären aber alle diese Ausdrücke für $\varkappa = 1, 2, \cdots n-1$ congruent 0, so erhielte man, da auch

$$\mathfrak{x}_1\mathfrak{x}_2 + \mathfrak{x}_2\mathfrak{x}_1 + \mathfrak{x}_3\mathfrak{x}_4 + \mathfrak{x}_4\mathfrak{x}_3 + \cdots + \mathfrak{x}_{n-1}\mathfrak{x}_n + \mathfrak{x}_n\mathfrak{x}_{n-1} \equiv 0$$

ist, für $\mathfrak{x}_1, \mathfrak{x}_2, \cdots \mathfrak{x}_n$ lauter gerade Werthe, was sie nicht sind. Man kann daher, gerade wie in nr. 5 des sechsten Capitels, ohne die erste Vertikalreihe der Substitution zu verändern, die Form φ weiter in eine äquivalente Form ψ überführen, welche, da $\omega_2 = 0$ ist, der Congruenz genügt:

$$(22) \qquad \psi \equiv 2(\alpha\mathfrak{x}^2 + \mathfrak{A}\mathfrak{x}\mathfrak{x}' + \mathfrak{a}\mathfrak{x}'^2) + f'(x_\varrho) \pmod{2^{t_0}},$$

worin $\mathfrak{A}$ eine beliebige ungerade Zahl ist; die Form $f'(x_\varrho)$ ist eine gegen 2 prime gerade Form, also $\sigma_1(f') = 2$, und nach den in jener nr. gegebenen Sätzen folgen die Beziehungen

$$\omega_{m-2}(f') = \omega_m(f)$$
$$\sigma_{m-2}(f') = \sigma_m(f)$$
$$(m = 3, 4, \cdots n-1)$$

sowie mittels des Hilfssatzes in nr. 8 daselbst folgende Congruenz:

$$(4\alpha\mathfrak{a} - \mathfrak{A}^2) \cdot \varDelta(f') \equiv \varDelta(f) \pmod{2^{t_0+1}}.$$

Ganz ebenso kann man g_0 in eine äquivalente Form χ verwandeln, für welche eine Congruenz

$$(23) \qquad \chi \equiv 2(\beta\mathfrak{x}^2 + \mathfrak{B}\mathfrak{x}\mathfrak{x}_1 + \mathfrak{b}\mathfrak{x}_1^2) + g'(x_\varrho) \pmod{2^{t_0}}$$

stattfindet, unter β irgend eine der ungeraden Zahlen verstanden, deren Doppeltes durch g_0 darstellbar ist, unter $\mathfrak{B}$ eine beliebige ungerade Zahl und unter $g'(x_\varrho)$ eine gegen 2 prime gerade Form. Aber man darf hier zunächst $2\beta \equiv 2\alpha$ voraussetzen, denn wegen der vorausgesetzten Gleichung (17) ist auch

$$f_0\{2\alpha, 2^{t_0}\} = g_0\{2\alpha, 2^{t_0}\}$$

d. h. zugleich mit

$$f_0(x_\varrho) \equiv 2\alpha \pmod{2^{\iota_0}}$$

ist auch

$$g_0(x_\varrho) \equiv 2\alpha \pmod{2^{\iota_0}}$$

erfüllbar.

Ferner darf man $\mathfrak{b} \equiv \mathfrak{a} \pmod{2}$ annehmen. Denn, wäre dies nicht der Fall, so könnte man zunächst, wenn nicht schon einer der Hauptcoefficienten von $g'(x_\varrho)$ congruent 2 (mod. 4) wäre, dies — wie an der angeführten Stelle auseinandergesetzt worden — durch eine Substitution, welche nur die Variabeln x_ϱ berührt und demnach die Gestalt der Congruenz (23) nicht ändert, erreichen; ist alsdann etwa der Coefficient $2c$ von x_i^2 congruent 2 (mod. 4), so würde die weitere Substitution

$$\mathfrak{x}_1 = \mathfrak{x}', \; x_i = \mathfrak{x}' + x_i'$$

und dann das Verfahren der nr. 5 des sechsten Capitels $\mathfrak{b}$ in

$$\mathfrak{b}' \equiv \mathfrak{b} + c \equiv \mathfrak{b} + 1 \pmod{2}$$

verwandeln, wo nun $\mathfrak{b}'$, wenn $\mathfrak{b}$ nicht $\equiv \mathfrak{a} \pmod{2}$ wäre, der Bedingung $\mathfrak{b}' \equiv \mathfrak{a} \pmod{2}$ genügt. Hiernach wird

$$4\beta\mathfrak{b} - \mathfrak{B}^2 \equiv 4\alpha\mathfrak{a} - \mathfrak{A}^2 \pmod{8}$$

vorausgesetzt werden dürfen, in Folge wovon es möglich wird, eine Zahl z der Congruenz

$$(24) \qquad 4\beta\mathfrak{b} - \mathfrak{B}^2 \equiv (4\alpha\mathfrak{a} - \mathfrak{A}^2)z^2 \pmod{2^{\iota_0+1}}$$

und eine andere z' der Congruenz

$$zz' \equiv 1 \pmod{2^{\iota_0+1}}$$

gemäss zu bestimmen. Da alsdann die Determinante

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & z' & 0 & \cdots & 0 \\ 0 & 0 & z & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} \equiv 1 \pmod{2^{\iota_0}}$$

ist, lässt sich eine unimodulare Substitution angeben (s. nr. 5 in Cap. 4), deren Coefficienten den Elementen dieser Determinante (mod. 2^{ι_0}) congruent sind, und durch sie geht offenbar χ in eine äquivalente Form χ' über, welche einer Congruenz

$$\chi' \equiv 2(\alpha\mathfrak{x}^2 + \mathfrak{B}z'\cdot\mathfrak{x}\mathfrak{x}' + \mathfrak{b}z'^2\cdot\mathfrak{x}'^2) + g'(x_\varrho) \pmod{2^{\iota_0}}$$

Genüge leistet. Wenn man hier ξ in $\xi + u\xi'$ verwandelt und u der Congruenz

$$2\alpha u + \mathfrak{B}z' \equiv \mathfrak{A} \pmod{2^{t_0+1}}$$

gemäss wählt, nimmt diese Congruenz die neue Gestalt an:

$$(25) \qquad \chi' \equiv 2(\alpha\xi^2 + \mathfrak{A}\xi\xi' + \mathfrak{a}\xi'^2) + g'(x_\varrho) \pmod{2^{t_0}},$$

wie aus (24) und $\beta \equiv \alpha \pmod{2^{t_0}}$ leicht hervorgeht.

Die Form $g'(x_\varrho)$ bedeutet in diesen Congruenzen wieder eine gegen 2 prime gerade Form, sodass $\sigma_1(g') = 2$ ist, während (wie in nr. 5 des sechsten Capitels) die Beziehungen

$$\omega_{m-2}(g') = \omega_m(g)$$
$$\sigma_{m-2}(g') = \sigma_m(g)$$
$$(m = 3, 4, \cdots n-1)$$

sowie aus dem Hilfssatze in nr. 8 daselbst die Congruenz

$$(4\alpha\mathfrak{a} - \mathfrak{A}^2) \cdot \varDelta(g') \equiv \varDelta(g) \pmod{2^{t_0+1}}$$

zu erschliessen sind. Nun folgt wieder, wie in den früheren Fällen, aus (17) die Gleichung

$$f'(h, 2^{t_0}) = g'(h, 2^{t_0}),$$

während die für f', g' schon gewonnenen Beziehungen die folgenden anderen Gleichungen

$$\omega_m(f') = \omega_m(g')$$
$$\sigma_m(f') = \sigma_m(g')$$
$$(m = 1, 2, \cdots n-3)$$

sowie die Congruenz

$$\varDelta(f') \equiv \varDelta(g') \pmod{2^{t_0+1}}$$

ergeben. Die Formen f', g' von nur $n-2$ Variabeln erfüllen demnach genau dieselben Voraussetzungen, wie die ursprünglichen Formen f, g von n Veränderlichen. Man gelangt somit zu der Folgerung: Ist der behauptete Satz richtig für zwei gerade Formen mit $n-2$ Veränderlichen, so folgt aus unseren bezüglich der Formen f, g gemachten Voraussetzungen $f' \simeq g' \pmod{2^{t_0}}$, es kann also g' durch eine nur die Veränderlichen x_ϱ betreffende und daher die Gestalt von (25) nicht ändernde Substitution in eine äquivalente Form g'' verwandelt werden, für welche $f' \equiv g'' \pmod{2^{t_0}}$ ist, und folglich χ' in eine äquivalente Form χ'', welche der Bedingung

$$\chi'' \equiv 2(\alpha\xi^2 + \mathfrak{A}\xi\xi' + \mathfrak{a}\xi'^2) + g''(x_\varrho)$$

also der Congruenz

$$\psi \equiv \chi'' \text{ (mod. } 2^{t_0})$$

Genüge leistet. Demnach gilt dann der Satz auch für zwei gerade Formen mit n Veränderlichen. Setzt man aber bei der voraufgehenden Betrachtung f, g als zwei solche Formen mit nur 2 Variabeln voraus, so erhalten die Congruenzen (22), (25) beide die Gestalt

$$\psi \equiv 2(\alpha\xi^2 + \mathfrak{A}\xi\xi' + \mathfrak{a}\xi'^2) \equiv \chi' \text{ (mod. } 2^{t_0})$$

und lehren somit unmittelbar die Giltigkeit des Satzes in diesem Falle, und folglich auch allgemein. —

5. Nachdem wir durch die Betrachtungen der letzten Nummern die Identität der neuen Definition eines Geschlechts von Formen mit der früheren nachgewiesen haben, können wir sie nunmehr etwas einfacher fassen. Nur dem Anscheine nach hängt die Zugehörigkeit einer Form zum Geschlechte von f nach dieser Definition von unendlich viel Kriterien, der Congruenz der Classen nach jedem beliebigen Modulus ab; wir dürfen ihnen die Congruenz nach dem einzigen Modulus 2Δ substituiren, wenn wir gleichzeitig die Form auf die Ordnung von f beschränken, und dürfen sagen: Diejenigen Classen von Formen derselben Ordnung wie f bilden das Geschlecht der Form f mit der Determinante Δ, welche mit der Classe von f (mod. 2Δ) congruent sind. In der That, da sie nach jedem Modulus ihr congruent sind, müssen sie es auch (mod. 2Δ); umgekehrt aber folgt aus ihrer Congruenz nach diesem Modulus (s. nr. 1), dass sie mit f, wie nach der Voraussetzung die Ordnung, so auch die Charaktere gemeinschaftlich haben, also dem gleichen Geschlechte angehörig sind.

Endlich lässt sich auch die Definition der Congruenz $f \simeq g$ (mod. N) zweier Classen auf eine andere, für die Folge zweckmässigere Weise fassen. Sind nämlich die Classen zweier Formen

$$f = \{a_{i\varkappa}\} \text{ und } g = \{b_{i\varkappa}\} \text{ (mod. } N)$$

congruent, so giebt es in der Classe von f eine Form $\varphi = \{\alpha_{i\varkappa}\}$, in der Classe von g eine Form $\psi = \{\beta_{i\varkappa}\}$, welche der Con-

gruenz
$$\{\alpha_{i\varkappa}\} \equiv \{\beta_{i\varkappa}\} \pmod{N}$$
genügen. Gehen diese Formen aus f resp. g durch die unimodularen Substitutionen $(q_{i\varkappa})$, $(r_{i\varkappa})$ hervor, sodass
$$(\alpha_{i\varkappa}) = (q_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (q_{i\varkappa})$$
$$(\beta_{i\varkappa}) = (r_{\varkappa i}) \cdot (b_{i\varkappa}) \cdot (r_{i\varkappa})$$
ist, so ergiebt sich, wenn unter $(\varrho_{i\varkappa})$ die inverse Substitution $(r_{i\varkappa})$ verstanden wird
$$(b_{i\varkappa}) = (\varrho_{\varkappa i}) \cdot (\beta_{i\varkappa}) \cdot (\varrho_{i\varkappa}) \equiv (\varrho_{\varkappa i}) \cdot (\alpha_{i\varkappa}) \cdot (\varrho_{i\varkappa}) \pmod{N}$$
also
$$(\varrho_{\varkappa i})(q_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (q_{i\varkappa})(\varrho_{i\varkappa}) \equiv (b_{i\varkappa}) \pmod{N}.$$
Es giebt mithin eine Substitution vom Modulus gleich 1, also auch congruent 1 (mod. N), welche $\{a_{i\varkappa}\}$ oder auch irgend einen Rest von $\{a_{i\varkappa}\}$ (mod. N) in einen Rest von $\{b_{i\varkappa}\}$ (mod. N) verwandelt.

Sei umgekehrt $\{\mathfrak{a}_{i\varkappa}\}$ irgend ein Rest von $\{a_{i\varkappa}\}$ (mod. N) und $(s_{i\varkappa})$ eine Substitution, deren Modulus $\equiv 1$ (mod. N) ist und welche $\{\mathfrak{a}_{i\varkappa}\}$ in einen Rest $\{\mathfrak{b}_{i\varkappa}\}$ von $\{b_{i\varkappa}\}$ verwandelt, so verwandelt sie e r s t e n s j e d e n Rest von $\{a_{i\varkappa}\}$ in einen Rest von $\{b_{i\varkappa}\}$. Z w e i t e n s kann man eine Substitution $(t_{i\varkappa})$ finden, deren Modulus g l e i c h 1 und welche $\equiv (s_{i\varkappa})$ (mod. N) ist. Sei dann
$$(t_{\varkappa i}) \cdot (a_{i\varkappa}) \cdot (t_{i\varkappa}) = (\alpha_{i\varkappa});$$
so folgt
$$(\alpha_{i\varkappa}) \equiv (s_{\varkappa i}) \cdot (\mathfrak{a}_{i\varkappa}) \cdot (s_{i\varkappa}) \equiv (\mathfrak{b}_{i\varkappa}) \equiv (b_{i\varkappa}) \pmod{N}$$
und somit giebt es eine Form der Classe von f, welche mit einer Form der Classe von g, nämlich mit g selbst, congruent ist, und folglich ist $f \simeq g$ (mod. N).

Aus beiden reciproken Ergebnissen schliesst man offenbar diese neue Definition für die Congruenz zweier Classen (mod. N):

Zwei Classen von Formen heissen einander (mod. N) congruent, wenn es eine Substitution giebt, deren Modulus $\equiv 1$ (mod. N) ist und durch welche die Reste der einen Classe in Reste der anderen übergehen.

6. An diese Definition für die Congruenz zweier Classen

(mod. N) schliessen wir die für die Folge erforderliche Untersuchung, wieviel Reste ein Geschlecht in Bezug auf einen gegebenen Modulus N haben kann.

Ist f der Repräsentant des Geschlechts, d. i. irgend eine in ihm enthaltene Form, so ist klar, dass die Reste dieses Geschlechts (mod. N) jedenfalls nur Reste solcher Formen φ sein können, für welche

$$f \simeq \varphi \pmod{N} \tag{26}$$

ist, denn die Formen φ des Geschlechts von f leisten der Congruenz $f \simeq \varphi$ in Bezug auf jeden Modulus, also auch (mod. N) Genüge. Ist aber φ eine solche Form, so muss der gedachten Definition zufolge f durch eine Substitution, deren Determinante $\equiv 1$ (mod. N) ist, in einen Rest von φ (mod. N) verwandelt werden. Mithin werden jedenfalls sämmtliche Reste des Geschlechts (mod. N) unter denjenigen zu finden sein, welche man erhält, wenn man auf f sämmtliche Substitutionen T, deren Determinante $\equiv 1$ (mod. N) ist, anwendet. Um die verschiedenen Reste zu finden, braucht man offenbar nur die incongruenten Substitutionen T zur Anwendung zu bringen. Angenommen nun, vermittelst dieser Substitutionen T finde man aus f die $\mathfrak{N}$ verschiedenen Reste

$$g_1, g_2, \cdots g_{\mathfrak{N}} \pmod{N},$$

so ist gewiss, dass das Geschlecht von f nicht mehr als diese $\mathfrak{N}$ Reste (mod. N) darbieten kann. Aber zudem sind sie auch wirklich vorhanden. Man sieht nämlich leicht ein, dass sie sogar schon von jeder Classe des Geschlechts z. B. von der Classe von f selbst geliefert werden. In der That, sind

$$T_1, T_2, \cdots T_{\mathfrak{N}}$$

solche Substitutionen T, durch welche f in die Formen $g_1, g_2, \cdots g_{\mathfrak{N}}$ (mod. N) übergeht, so lassen sich ebenso viel verschiedene Substitutionen $S_1, S_2, \cdots S_{\mathfrak{N}}$ bilden, welche jenen (mod. N) congruent sind und den Modulus 1 haben, und offenbar geben die vermittelst derselben aus f hervorgehenden Formen der Classe von f die Reste $g_1, g_2, \cdots g_{\mathfrak{N}}$ (mod. N).

Zur Ermittelung der Zahl $\mathfrak{N}$ suchen wir vor Allem die Anzahl der incongruenten Substitutionen

(27) $$T = (t_{i\varkappa}),\quad (i, \varkappa = 1, 2, \cdots n)$$

deren Modulus $\equiv 1 \pmod{N}$ ist. Um sie alle zu finden, denke man den Zahlen

(28) $$r_1, r_2, \cdots r_n$$

alle Reste (mod. N) beigelegt, was N^n Restsysteme ergiebt; die Zahlen eines jeden dieser Restsysteme haben mit N einen grössten gemeinsamen Theiler d, und wir wollen alle Restsysteme, denen derselbe Theiler d zukommt, in einen Complex zusammengefasst denken und ihre Anzahl mit $\Phi(d)$ bezeichnen; offenbar ist dann die auf sämmtliche Theiler d von N bezogene Summe

$$\sum_d \Phi(d) = N^n$$

und hieraus schliesst man in bekannter Weise die Gleichung

$$\Phi(1) = N^n \cdot \prod_q \left(1 - \frac{1}{q^n}\right),$$

in welcher die Multiplikation auf alle verschiedenen Primfaktoren von N zu erstrecken ist. Setzen wir zur Abkürzung

(29) $$\prod_q \left(1 - \frac{1}{q^n}\right) = (N)_n,$$

so können wir einfacher schreiben

(30) $$\Phi(1) = N^n \cdot (N)_n.$$

Diese Formel bestimmt die Anzahl der Restsysteme (28) (mod. N), welche ohne gemeinsamen Theiler sind, mit N. Eins dieser $\Phi(1)$ Restsysteme müssen aber die Zahlen $t_{11}, t_{21}, \cdots t_{n1}$ (mod. N) lassen, damit sie die erste Vertikalreihe der Coefficienten einer Substitution (27), deren Determinante $\equiv 1 \pmod{N}$ ist, bilden können. Und umgekehrt, so oft die Zahlen $r_1, r_2, \cdots r_n$ eins dieser Restsysteme bilden, giebt es eine Substitution (27) von der gedachten Art, in welcher die Elemente der ersten Vertikalreihe ihnen congruent sind; denn, weil $r_1, r_2, \cdots r_n$ keinen Theiler mit N gemeinsam haben, giebt es auch Zahlen

$$t_{11} \equiv r_1,\ t_{21} \equiv r_2,\ \cdots t_{n1} \equiv r_n \pmod{N},$$

welche überhaupt ohne gemeinsamen Theiler sind, und jede

unimodulare Substitution, in welcher sie die erste Vertikalreihe bilden, ist eine Substitution T von der behaupteten Beschaffenheit.

Aus einer solchen Substitution mit der ersten Vertikalreihe $t_{11}, t_{21}, \cdots t_{n1}$ erhält man aber jede andere von derselben Beschaffenheit, wie man unschwer erkennt, dadurch, dass man sie mit sämmtlichen (mod. N) incongruenten Substitutionen

$$U = \begin{pmatrix} 1, & U_1, & U_2, & \cdots U_{n-1} \\ 0, & u_{11}, & u_{12}, & \cdots u_{1,n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & u_{n-1,1}, & u_{n-1,2}, & \cdots u_{n-1,n-1} \end{pmatrix}$$

zusammensetzt, für welche die Determinante $n-1^{\text{ten}}$ Grades $|u_{i\varkappa}| \equiv 1$ (mod. N) ist. Bezeichnen wir nun allgemein mit $\psi_n(N)$ die Anzahl der incongruenten Substitutionen $(t_{i\varkappa})$, deren Determinante n^{ten} Grades $|t_{i\varkappa}| \equiv 1$ (mod. N) ist, also mit $\psi_{n-1}(N)$ die Anzahl der incongruenten Substitutionen $(u_{i\varkappa})$ mit dem Modulus $|u_{i\varkappa}| \equiv 1$ (mod. N), so ist, da die Zahlen $U_1, U_2, \cdots U_{n-1}$ (mod. N) jeden Rest haben können, die Anzahl der incongruenten U und folglich auch die der Substitutionen T mit der ersten Vertikalreihe $t_{11}, t_{21}, \cdots t_{n1}$ gleich $N^{n-1} \cdot \psi_{n-1}(N)$. Daher beläuft sich die gesammte Anzahl der incongruenten Substitutionen T, die wir suchen, auf

$$N^n (N)_n \cdot N^{n-1} \psi_{n-1}(N)$$

und somit erhalten wir die Recursionsformel

$$\psi_n(N) = N^{2n-1} \cdot (N)_n \cdot \psi_{n-1}(N)$$

aus welcher sich sodann, da $\psi_1(N)$ offenbar gleich 1 ist,

$$(31) \qquad \psi_n(N) = N^{n^2-1} \cdot (N)_2 (N)_3 \cdots (N)_n$$

ergiebt*).

Wenn wir nun alle diese Substitutionen T auf die Form $f \equiv g_1$ (mod. N) zur Anwendung bringen, so mögen diejenigen von ihnen, welche f in eine mit g_1 (mod. N) congruente Form verwandeln und zu denen die identische Substitution zählt, mit T und ihre Anzahl mit $f(N)$ bezeichnet werden. Ebenso viel Substitutionen T liefern dann für f eine mit g_2, ebenso viel

*) Vgl. hierzu C. Jordan, traité des substitutions, art. 120—124.

eine mit g_3 (mod. N) congruente Form u. s. w. Denn, ist T_0 eine Substitution T, welche $f \equiv g_1$ in eine Form verwandelt, deren Rest g_2 ist, so wird auch $\mathsf{T} \cdot T_0$ eine solche sein; und umgekehrt, wenn T_1 noch eine andere Substitution T ist, welche dies bewirkt, so wird auch die mit T_0 (mod. N) congruente unimodulare Substitution S_0 von derselben Art sein, die umgekehrte Substitution S_0^{-1} also wird g_2, und die Substitution $T_1 S_0^{-1}$ wird f in eine mit f oder g_1 (mod. N) congruente Form verwandeln d. h. es wird

$$T_1 S_0^{-1} \equiv \mathsf{T},\ T_1 \equiv \mathsf{T} S_0 \equiv \mathsf{T} T_0 \pmod{N}$$

sein; in der That ist also die Anzahl der incongruenten Substitutionen T, welche $f \equiv g_2$ liefern, gleich derjenigen der Substitutionen T. Hieraus aber folgt offenbar

$$\psi_n(N) = \mathfrak{N} \cdot f(N)$$

und somit

$$\mathfrak{N} = \frac{\psi_n(N)}{f(N)}. \tag{32}$$

7. Zur Bestimmung von $\mathfrak{N}$ handelt es sich also noch um Ermittelung des Werthes der Funktion $f(N)$.

Hierzu bemerken wir vor Allem, dass dieser Werth sich finden lässt, indem man die Funktion nur für solche Argumente bestimmt, welche Primzahlpotenzen sind. Ist nämlich

$$N = p^t \cdot p'^{t'} \cdots, \tag{33}$$

so ist

$$f(N) = f(p^t) \cdot f(p'^{t'}) \cdots. \tag{34}$$

In der That, ist eine Substitution $T = (t_{i\varkappa})$ mit der Determinante $| t_{i\varkappa} | \equiv 1$ (mod. N) so beschaffen, dass

$$(t_{\varkappa i}) \cdot f \cdot (t_{i\varkappa}) \equiv g_1 \pmod{N}$$

ist, so ist sie zugleich auch eine Substitution, deren Determinante $\equiv 1$ (mod. p^t) und für welche

$$(t_{\varkappa i}) \cdot f \cdot (t_{i\varkappa}) \equiv g_1 \pmod{p^t}$$

ist, und eben dasselbe gilt für die übrigen Primzahlpotenzen von N. Aber auch umgekehrt, wenn

$$S = (s_{i\varkappa}),\ S' = (s'_{i\varkappa}), \cdots$$

Substitutionen sind, deren Determinanten resp.

$$(\text{mod. } p^t),\ (\text{mod. } p'^{t'}), \cdots$$

hierbei ist, wenn wieder $\vartheta_i - \vartheta_{i-1} = \varkappa_i$ gesetzt wird,

$$\Phi_i = \alpha_i x_1^{(i)2} + \alpha_i' x_2^{(i)2} + \cdots + \alpha_i^{(\varkappa_i - 1)} x_{\varkappa_i}^{(i)2}.$$

Demnach darf man auch schreiben:

$$f \equiv \alpha_1 x_1'^2 + p^{\omega_1} \cdot f'(x_\varrho') \pmod{p^t}, \tag{38}$$

wo $f'(x_\varrho')$ eine Form von $n-1$ Veränderlichen ist, für deren Invarianten die Beziehungen bestehen:

$$\omega'_{m-1} = \omega_m.$$
$$(m = 2, 3, \cdots n-1)$$

Ist nun $\mathsf{T} = (t_{i\varkappa})$ eine Substitution, welche $f(x_\varrho) \pmod{p^t}$ nicht verändert, so müssen die Elemente der ersten Vertikalreihe $t_{11}, t_{21}, \cdots t_{n1}$ eine Wurzel der Congruenz

$$f(x_\varrho) \equiv \alpha_1 \pmod{p^t} \tag{39}$$

sein. Die Anzahl der Wurzeln derselben beträgt nach 1, 1) vorigen Capitels

$$\mathsf{A} \cdot p^{(n-1)(t-1)}$$

wenn A die Anzahl der Wurzeln der Congruenz

$$f(x_\varrho) \equiv \alpha_1 x_1^2 + \alpha_1' x_2^2 + \cdots + \alpha_1^{(\varkappa_1 - 1)} x_{\varkappa_1}^2 \equiv \alpha_1 \pmod{p} \tag{40}$$

bezeichnet. Ist umgekehrt $t_{11}, t_{21}, \cdots t_{n1}$ eine Wurzel derselben, so entspricht ihr, wie in nr. 2 gezeigt worden, eine unimodulare Substitution, in welcher $t_{11}, t_{21}, \cdots t_{n1}$ die erste Vertikalreihe bilden und durch welche $f(x_\varrho)$ in eine äquivalente Form ψ von der Beschaffenheit übergeht, dass

$$\psi \equiv \alpha_1 \xi_1^2 + p^{\omega_1} \cdot f''(\xi_\varrho) \pmod{p^t}$$

und $f''(\xi_\varrho)$ eine Form von $n-1$ Veränderlichen ist, für welche die Beziehungen

$$\omega''_{m-1} = \omega_m$$
$$(m = 2, 3, \cdots n-1)$$

erfüllt sind. Da somit die Gleichungen

$$\omega'_{m-1} = \omega''_{m-1}$$
$$(m = 2, 3, \cdots n-1)$$

stattfinden und für $t' = t - \omega_1$ leicht auch die anderen

$$f'(h, p^{t'}) = f''(h, p^{t'})$$

$$\Delta(f') \equiv \Delta(f'') \pmod{p^{t' + \partial'_n - 2}}$$

erschlossen werden, so ergiebt sich nach den Sätzen jener nr.

die Congruenz

$$f''(\xi_\varrho) \simeq f'(x_\varrho') \pmod{p^{t'}}$$

d. h. man kann auf ψ eine, die Veränderliche ξ_1 nicht berührende unimodulare Substitution anwenden, durch welche $f''(\xi_\varrho)$ in eine Form übergeht, die (mod. $p^{t'}$) den Rest $f'(x_\varrho')$ giebt. Durch Zusammensetzung dieser Substitution mit derjenigen, durch welche ψ aus f hervorging, gewinnt man folglich eine Substitution T mit der ersten Vertikalreihe

$$t_{11}, t_{21}, \cdots t_{n1},$$

welche f (mod. p^t) ungeändert lässt.

Alle anderen Substitutionen T, welche dieselbe erste Vertikalreihe haben, müssen aus dieser einen hervorgehen, indem man sie mit Substitutionen von der Form U zusammensetzt, die ihrerseits sich als Produkt zweier Substitutionen von der Form

$$\begin{pmatrix} 1 & U_1 & \cdots & U_{n-1} \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & u_{11} & \cdots & u_{1,n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & u_{n-1,1} & \cdots & u_{n-1,n-1} \end{pmatrix}$$

darstellen.

Soll aber $\mathrm{T} \cdot U$ den Rest von f (mod. p^t) nicht ändern, so darf auch U selbst es nicht, woraus wegen der Form dieser Substitution und weil in $f(x_\varrho)$ die Coefficienten der doppelten Produkte, welche x_1 enthalten, durch p^t theilbar sind, sich leicht

$$U_1 \equiv U_2 \equiv \cdots \equiv U_{n-1} \equiv 0 \pmod{p^t}$$

ergiebt; und hieraus wird ersichtlich, dass U dann und nur dann den Rest von f (mod. p^t) nicht verändert, wenn die Substitution $(u_{i\varkappa})$ die Form $p^{\omega_1} \cdot f'$ (mod. p^t) nicht verändert. Aus diesen Betrachtungen folgt, dass zu jeder Wurzel $t_{11}, t_{21}, \cdots t_{n1}$ der Congruenz (39) soviel Substitutionen T, welche sämmtlich diese Zahlen als erste Vertikalreihe haben, gehören, als die Anzahl der gedachten Substitutionen $(u_{i\varkappa})$ beträgt d. i. mit Rücksicht auf (36)

$$p^{((n-1)^2-1)\omega_1} \cdot f'(p^{t-\omega_1}).$$

In Folge hiervon erhält man die Recursionsformel:

$$(41)\qquad f(p^t) = \mathsf{A}\cdot p^{[(n-1)^2-1]\omega_1+(n-1)(t-1)}\cdot f'(p^{t-\omega_1}).$$

Da für eine Form f mit nur einer Veränderlichen $\mathsf{A}=2$, offenbar aber $f(p^t)=1$ ist, wäre in vorstehender Formel alsdann statt des letzten Faktors $\frac{1}{2}$ zu setzen.

Schreibt man nun in analoger Weise

$$f'(x_\varrho') \equiv \alpha_1' x_2'^2 + p^{\omega_2}\cdot f^{(2)}(x_\varrho') \pmod{p^{t-\omega_1}}$$

u. s. w., sodass

$$(42)\quad f^{(\varkappa_1)}(x_\varrho) \equiv \Phi_2 + p^{\omega\vartheta_2}\cdot\Phi_3 + \cdots + p^{\omega\vartheta_2+\cdots+\omega\vartheta_{\lambda-1}}\cdot\Phi_\lambda \pmod{p^{t-v\vartheta_1}}$$

wird, und bezeichnet man mit $\mathsf{A}_1, \mathsf{A}_2, \cdots \mathsf{A}_{\varkappa_1-1}$ die Anzahl der Wurzeln der Congruenzen

$$\begin{array}{lll} f'(x_\varrho) & \equiv \alpha_1' x_2^2 + \alpha_1'' x_3^2 + \cdots + \alpha_1^{(\varkappa_1-1)} x_{\varkappa_1}^2 & \equiv \alpha_1' \\ f''(x_\varrho) & \equiv \qquad\qquad \alpha_1'' x_3^2 + \cdots + \alpha_1^{(\varkappa_1-1)} x_{\varkappa_1}^2 & \equiv \alpha_1'' \\ \cdots & \cdots & \cdots \\ f^{(\varkappa_1-1)}(x_\varrho) & \equiv \qquad\qquad\qquad\qquad \alpha_1^{(\varkappa_1-1)} x_{\varkappa_1}^2 & \equiv \alpha_1^{(\varkappa_1-1)} \end{array} \pmod{p}$$

resp., so ergeben sich neben der Formel (41) die ähnlichen, welche folgen:

$$f'(p^{t-\omega_1}) = \mathsf{A}_1\cdot p^{[(n-2)^2-1]\omega_2+(n-2)(t-1-\omega_1)}\cdot f^{(2)}(p^{t-\omega_1-\omega_2})$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f^{(\varkappa_1-1)}(p^{t-\omega_1-\cdots-\omega_{\varkappa_1-1}})$$

$$= \mathsf{A}_{\varkappa_1-1}\cdot p^{[(n-\varkappa_1)^2-1]\omega_{\varkappa_1}+(n-\varkappa_1)(t-1-\omega_1-\cdots-\omega_{\varkappa_1-1})}\cdot f^{(\varkappa_1)}(p^{t-v\vartheta_1}),$$

Gleichungen, welche durch Multiplikation unter sich und mit (41) verbunden, da $\omega_1, \omega_2, \cdots \omega_{\varkappa_1-1}$ Null sind, die folgende ergeben:

$$(43)\qquad \left\{\begin{array}{l} f(p^t) = \mathsf{A}\cdot\mathsf{A}_1\cdot\mathsf{A}_2\cdots\mathsf{A}_{\varkappa_1-1} \\ \cdot\, p^{\left(\frac{n(n-1)}{2}-\frac{(n-\varkappa_1)(n-\varkappa_1-1)}{2}\right)(t-1)+[(n-\varkappa_1)^2-1]\omega\vartheta_1} \\ \cdot\, f^{(\varkappa_1)}(p^{t-v\vartheta_1}). \end{array}\right.$$

Ist nun zuerst $\varkappa_1$ gerade, so findet sich aus den Schlussformeln von nr. 2 vorigen Capitels, wenn man zur Abkürzung

$$\left(\frac{(-1)^{\frac{\varkappa_1}{2}}\cdot\alpha_1\alpha_1'\cdots\alpha_1^{(\varkappa_1-1)}}{p}\right) = \theta$$

setzt,

$$\mathsf{A} \quad = p^{n-1}\left[1 - p^{-\frac{\varkappa_1}{2}} \cdot \theta\right]$$

$$\mathsf{A}_1 \quad = p^{n-2}\left[1 + p^{-\frac{\varkappa - 2}{2}} \cdot \theta \cdot \left(\frac{-\alpha_1 \alpha_1'}{p}\right)\right]$$

$$\mathsf{A}_2 \quad = p^{n-3}\left[1 - p^{-\frac{\varkappa_1 - 2}{2}} \cdot \theta \cdot \left(\frac{-\alpha_1 \alpha_1'}{p}\right)\right]$$

$$\mathsf{A}_3 \quad = p^{n-4}\left[1 + p^{-\frac{\varkappa_1 - 4}{2}} \cdot \theta \cdot \left(\frac{\alpha_1 \alpha_1' \alpha_1'' \alpha_1'''}{p}\right)\right]$$

. . . .

$$\mathsf{A}_{\varkappa_1 - 1} = p^{n-\varkappa_1}\left[1 + \theta \cdot \left(\frac{(-1)^{\frac{\varkappa_1}{2}} \alpha_1 \alpha_1' \cdots \alpha_1^{(\varkappa_1 - 1)}}{p}\right)\right]$$

d. i. gleich $2p^{n-\varkappa_1}$,

mithin

$$\mathsf{A} \cdot \mathsf{A}_1 \cdot \mathsf{A}_2 \cdots \mathsf{A}_{\varkappa_1 - 1}$$

$$= p^{\frac{n(n-1)}{2} - \frac{(n-\varkappa_1)(n-\varkappa_1-1)}{2}} \cdot 2\left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right) \cdots$$

$$\cdots \left(1 - \frac{1}{p^{\varkappa_1 - 2}}\right) \cdot \left(1 - \frac{\theta}{p^{\frac{\varkappa_1}{2}}}\right).$$

Ist dagegen $\varkappa_1$ ungerade, so ergeben sich, wenn man

$$\left(\frac{(-1)^{\frac{\varkappa_1 - 1}{2}} \cdot \alpha_1' \alpha_1'' \cdots \alpha_1^{(\varkappa_1 - 1)}}{p}\right) = \theta_1$$

setzt, auf gleiche Weise

$$\mathsf{A} \quad = p^{n-1}\left[1 + p^{-\frac{\varkappa_1 - 1}{2}} \cdot \theta_1\right]$$

$$\mathsf{A}_1 \quad = p^{n-2}\left[1 - p^{-\frac{\varkappa_1 - 1}{2}} \cdot \theta_1\right]$$

$$\mathsf{A}_2 \quad = p^{n-3}\left[1 + p^{-\frac{\varkappa_1 - 3}{2}} \cdot \theta_1 \left(\frac{-\alpha_1' \alpha_1''}{p}\right)\right]$$

. . . .

$$\mathsf{A}_{\varkappa_1 - 2} = p^{n-\varkappa_1+1}\left[1 - p^{-1} \cdot \theta_1 \cdot \left(\frac{(-1)^{\frac{\varkappa_1 - 3}{2}} \alpha_1' \alpha_1'' \cdots \alpha_1^{(\varkappa_1 - 3)}}{p}\right)\right]$$

$$\mathsf{A}_{\varkappa_1 - 1} = p^{n-\varkappa_1}\left[1 + \theta_1 \cdot \left(\frac{(-1)^{\frac{\varkappa_1 - 1}{2}} \alpha_1' \alpha_1'' \cdots \alpha_1^{(\varkappa_1 - 1)}}{p}\right)\right]$$

d. i. gleich $2p^{n-\varkappa_1}$,

mithin

$$A\cdot A_1\cdot A_2\cdots A_{\varkappa_1-1}$$
$$=p^{\frac{n(n-1)}{2}-\frac{(n-\varkappa_1)(n-\varkappa_1-1)}{2}}\cdot 2\left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^4}\right)\cdots\left(1-\frac{1}{p^{\varkappa_1-1}}\right).$$

Diese beiden Formeln lassen sich vereinen, wenn man, jenachdem $\varkappa_1$ gerade oder ungerade ist

$$(44)\qquad \mathfrak{a}_{\varkappa_1}=1-\left(\frac{(-1)^{\frac{\varkappa_1}{2}}\alpha_1\alpha_1'\cdots\alpha_1^{(\varkappa_1-1)}}{p}\right)\cdot p^{-\frac{\varkappa_1}{2}}\text{ oder }=1$$

setzt; dann findet sich allgemein

$$(45)\qquad \begin{cases} A\cdot A_1\cdot A_2\cdots A_{\varkappa_1-1} \\ =p^{\frac{n(n-1)}{2}-\frac{(n-\varkappa_1)(n-\varkappa_1-1)}{2}}\cdot 2\left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^4}\right)\cdots \\ \cdots\left(1-\frac{1}{p^{2\left[\frac{\varkappa_1-1}{2}\right]}}\right)\cdot\mathfrak{a}_{\varkappa_1}. \end{cases}$$

Durch Einsetzen dieses Werthes in die Formel (43) ergiebt sich die Recursionsformel:

$$(46)\qquad \begin{cases} f(p^t)=2\,\mathfrak{P}_1\cdot p^{\left(\frac{n(n-1)}{2}-\frac{(n-\varkappa_1)(n-\varkappa_1-1)}{2}\right)t+[(n-\varkappa_1)^2-1]\omega\vartheta_1} \\ \cdot f^{(\varkappa_1)}\left(p^{t-\nu\vartheta_1}\right), \end{cases}$$

in welcher zur Abkürzung

$$(47)\qquad \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^4}\right)\cdots\left(1-\frac{1}{p^{2\left[\frac{\varkappa_1-1}{2}\right]}}\right)\cdot\mathfrak{a}_{\varkappa_1}=\mathfrak{P}_1$$

gesetzt worden ist. Verfährt man nun bezüglich der Form $f^{(\varkappa_1)}(x_\varrho)$ auf Grund der Congruenz (42) ganz analog, wie auf Grund von (37) mit der Form $f(x_\varrho)$ geschah, und fährt so fort, so gelangt man mit Beachtung der zu Formel (41) hinzugefügten Bemerkung ohne weitere Schwierigkeit zu einer Formel von folgender Gestalt:

$$(48)\qquad f(p^t)=p^{\frac{n(n-1)}{2}t+\sum_{h=1}^{n-1}\left(\frac{(n-h)(n-h+1)}{2}-1\right)\omega_h}\cdot f[p],$$

wo

$$(49)\qquad f[p]=2^{\lambda-1}\cdot\mathfrak{P}_1\,\mathfrak{P}_2\cdots\mathfrak{P}_\lambda$$

gesetzt und $\mathfrak{P}_i$ aus der Form Φ_i zu bilden ist, wie $\mathfrak{P}_1$ aus der Form Φ_1.

9. Es handle sich jetzt zweitens um die Bestimmung von $f(2^t)$, wobei $t > 1 + v_{n-1}$ vorausgesetzt wird. Auch hier darf man unter f eine charakteristische Form der Classe von f verstehen. Man muss aber die beiden Fälle unterscheiden, ob $\sigma_1 = 1$ oder $= 2$ ist.

Erster Fall: $\sigma_1 = 1$. Die Form $f(x_\varrho)$ genügt alsdann einer Congruenz

$$(50)\qquad f(x_\varrho) \equiv \alpha x_1^2 + \alpha' x_2^2 + \cdots + \alpha^{(n-1)} x_n^2 \pmod{2^t},$$

in welcher die Coefficienten $\alpha, \alpha', \cdots \alpha^{(n-1)}$ ungerade sind, eine Congruenz, der man, da die ω_i sämmtlich Null sind, auch folgende Gestalt geben kann:

$$(51)\qquad f(x_\varrho) \equiv \alpha x_1^2 + 2^{\omega_1} \cdot f'(x_\varrho) \pmod{2^t},$$

indem man unter $f'(x_\varrho)$ die Form

$$(52)\qquad f'(x_\varrho) \equiv \alpha' x_2^2 + \cdots + \alpha^{(n-1)} x_n^2 \pmod{2^t}$$

versteht. Soll nun $\mathsf{T} = (t_{i\varkappa})$ eine Substitution sein, deren Determinante $\equiv 1 \pmod{2^t}$ und welche $f \pmod{2^t}$ nicht verändert, so müssen jedenfalls die Elemente $t_{11}, t_{21}, \cdots t_{n1}$ der ersten Vertikalreihe die Congruenz

$$(53)\qquad f(x_\varrho) \equiv \alpha \pmod{2^t}$$

erfüllen und folgende andere Congruenzen:

$$\left.\begin{aligned} \alpha \cdot t_{11} t_{1h} + \alpha' \cdot t_{21} t_{2h} + \cdots + \alpha^{(n-1)} t_{n1} t_{nh} &\equiv 0 \\ \alpha \cdot t_{1h}^2 + \alpha' \cdot t_{2h}^2 + \cdots + \alpha^{(n-1)} t_{nh}^2 &\equiv 1 \end{aligned}\right\} \pmod{2}$$

d. i.

$$\begin{aligned} t_{11} t_{1h} + t_{21} t_{2h} + \cdots + t_{n1} t_{nh} &\equiv 0 \\ t_{1h} + t_{2h} + \cdots + t_{nh} &\equiv 1 \end{aligned}$$

und folglich

$$(t_{11} - 1) t_{1h} + (t_{21} - 1) t_{2h} + \cdots + (t_{n1} - 1) t_{nh} \equiv 1 \pmod{2}$$

bestehen, woraus hervorgeht, dass die Zahlen $t_{11}, t_{21}, \cdots t_{n1}$ nicht sämmtlich ungerade sein dürfen. Man überzeugt sich nun auf ganz dieselbe Weise, wie im vorigen Falle, wobei man sich nur auf nr. 3 statt auf nr. 2 zu stützen hat, dass in der That jeder Wurzel der Congruenz (53) in nicht lauter ungeraden Zahlen $t_{11}, t_{21}, \cdots t_{n1}$ eine der Substitutionen T ent-

spricht, welche diese Zahlen als erste Vertikalreihe hat. Wenn man zudem bedenkt, dass nach nr. 1, 2) und nr. 3 des siebenten Capitels die Anzahl der bezeichneten Wurzeln gleich $2^{(n-1)(t-2)}$ mal der Anzahl $\mathfrak{A}$ der Wurzeln der Congruenz

$$(54)\qquad \alpha x_1^2 + \alpha' x_2^2 + \cdots + \alpha^{(n-1)} x_n^2 \equiv \alpha \pmod{4}$$

in nicht lauter ungeraden Zahlen ist, gelangt man auf solche Weise wieder zur folgenden Recursionsformel:

$$(55)\qquad f(2^t) = 2^{(n-1)(t-2)} \cdot \mathfrak{A} \cdot f'(2^t).$$

Ist nun zunächst n gerade, so bezeichnet $\mathfrak{A}$ die Anzahl der sämmtlichen Wurzeln der Congruenz (54), ist also (s. die Tabelle in nr. 4 des angeführten Capitels),

wenn $\varepsilon = +1$ ist, gleich $2^{2(n-1)}$, dagegen, wenn $\varepsilon = -1$ ist, gleich

$$2^{2(n-1)} \cdot \left(1 - \frac{(-1)^{\frac{\alpha-1}{2}} \delta}{2^{\frac{n}{2}-1}}\right),$$

und somit kommt für ein gerades n:

$$(56a)\qquad f(2^t) = 2^{(n-1)t} \cdot \left(1 + (\varepsilon - 1) \cdot \frac{(-1)^{\frac{\alpha-1}{2}} \delta}{2^{\frac{n}{2}}}\right) \cdot f'(2^t).$$

Ist dagegen n ungerade, so hat man zwei Fälle zu unterscheiden, jenachdem

entweder

$$\left.\begin{array}{l} \varepsilon \equiv \alpha + \alpha' + \cdots + \alpha^{(n-1)} \equiv -\alpha \\ \text{oder} \\ \varepsilon \equiv \alpha + \alpha' + \cdots + \alpha^{(n-1)} \equiv +\alpha \end{array}\right\} \pmod{4}$$

ist. Im ersteren Falle bezeichnet wieder $\mathfrak{A}$ die Anzahl sämmtlicher Wurzeln der Congruenz (54), ist also nach der genannten Tabelle gleich

$$2^{2(n-1)} \cdot \left(1 - \frac{\delta}{2^{\frac{n-1}{2}}}\right);$$

im zweiten dagegen ist $\mathfrak{A}$ gleich dem Unterschiede zwischen der Anzahl sämmtlicher Wurzeln und der Anzahl der Wurzeln in lauter ungeraden Zahlen, d. i.

$$2^{2(n-1)}\cdot\left(1+\frac{\delta}{2^{\frac{n-1}{2}}}-\frac{1}{2^{n-2}}\right)$$
$$=2^{2(n-1)}\cdot\left(1-\frac{\delta}{2^{\frac{n-1}{2}}}\right)\left(1+\frac{\delta}{2^{\frac{n-3}{2}}}\right).$$

Beide Fälle fassen sich zusammen in eine einzige Formel und geben für ein ungerades n:

$$(56\text{b})\quad \begin{cases} f(2^t)=2^{(n-1)t}\cdot\left(1-\dfrac{\delta}{2^{\frac{n-1}{2}}}\right) \\ \qquad\cdot\left(1+\left(1+\varepsilon\cdot(-1)^{\frac{\alpha-1}{2}}\right)\dfrac{\delta}{2^{\frac{n-1}{2}}}\right)\cdot f'(2^t). \end{cases}$$

Zudem bestehen nach Ende von nr. 4 des siebenten Capitels folgende Relationen:

$$(57)\quad \varepsilon_1=(-1)^{n-1+\frac{\alpha-1}{2}}\cdot\varepsilon,\ \delta_1=(-1)^{n\cdot\frac{\alpha-1}{2}}\cdot\varepsilon^{n-1+\frac{\alpha-1}{2}}\cdot\delta,$$

welche den Uebergang von der Form f mit n Veränderlichen zu der Form f' mit $n-1$ Veränderlichen vermitteln. Indem man nun abwechselnd eine und die andere der Formeln (56a) und (56b) verwendet und die Beziehungen (57) für die neu entstehenden Formen fortsetzt, wobei man, ohne die Allgemeinheit zu beschränken, der Einfachheit wegen annehmen kann, dass die ersten μ Coefficienten α von der Form $4j+1$, die letzten ν von der Form $4j+3$ sind, gelangt man — wie durch den Schluss von $n-1$ auf n leicht zu bestätigen ist — zu folgendem Resultat:

$$(58)\qquad f(2^t)=2^{\frac{n(n-1)}{2}t}\cdot f[2],$$

wo zur Abkürzung

$$(59)\quad f[2]=2\cdot\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{2^4}\right)\cdots\left(1-\frac{1}{2^{2\left[\frac{n-1}{2}\right]}}\right)\cdot\mathfrak{b}_1$$

gesetzt ist, und,

wenn n gerade und $\varepsilon=+1$ ist, $\mathfrak{b}_1=\left(1+\dfrac{\delta}{2^{\frac{n}{2}-1}}\right)^{-1}$

„ „ „ „ $\varepsilon=-1$ ist, $\mathfrak{b}_1=1$

wenn n ungerade ist

$$\mathfrak{b}_1 = \left(1 + \frac{\delta}{2^{\frac{n-1}{2}}}\right)^{-1}$$

gewählt werden muss.

10. Zweiter Fall: $\sigma_1 = 2$. In diesem Falle, der ein gerades n erfordert, darf man für f folgende Congruenz voraussetzen:

$$(60) \quad f(x_\varrho) \equiv \sum_{i=1}^{\frac{n}{2}} (2\alpha_i x_i^2 + 2\mathfrak{A}_i x_i x_i' + 2\mathfrak{a}_i x_i'^2) \pmod{2^\iota},$$

in welcher die Zahlen α_i, $\mathfrak{A}_i$ ungerade sind, eine Congruenz, der man auch, da die sämmtlichen ω gleich Null sind, diese Form geben kann:

$$(61) \quad f(x_\varrho) \equiv 2\alpha_1 x_1^2 + 2\mathfrak{A}_1 x_1 x_1' + 2\mathfrak{a}_1 x_1'^2 + 2^{\omega_2} \cdot f_2(x_\varrho) \pmod{2^\iota},$$

indem man unter $f_2(x_\varrho)$ eine gerade Form versteht von nur $n-2$ Veränderlichen, unter denen x_1, x_1' sich nicht mehr finden. Soll nun $\mathsf{T} = (t_{i\varkappa})$ eine Substitution sein, deren Modulus $\equiv 1 \pmod{2^\iota}$ und welche $f \pmod{2^\iota}$ nicht verändert, so muss die Congruenz

$$(62) \qquad f(x_\varrho) \equiv 2\alpha_1 \pmod{2^\iota}$$

durch die Elemente $t_{11}, t_{21}, \cdots t_{n1}$ ihrer ersten Vertikalreihe erfüllt werden; sie können demnach nicht sämmtlich gerade Zahlen sein. Bezeichnen aber diese Elemente irgend eine Wurzel der vorstehenden Congruenz, so folgt ganz wie in nr. 5 des 6. Cap. (vgl. nr. 4), dass durch eine unimodulare Substitution, bei welcher jene Zahlen die erste Vertikalreihe bilden, und durch eine Reihe von anderen, welche diese Vertikalreihe nicht verändern, $f(x_\varrho)$ in eine äquivalente Form $\psi(x_\varrho)$ transformirt werden kann, welche einer Congruenz genügt von der Gestalt:

$$2\alpha_1 \cdot \psi(x_\varrho) \equiv (2\alpha_1 x_1 + \mathfrak{A}_1 x_1')^2 + (4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2)x_1'^2 + 2\alpha_1 \cdot f^{(2)}(x_\varrho) \pmod{2^{\iota+1}},$$

während

$$(63) \quad 2\alpha_1 \cdot f(x_\varrho) \equiv (2\alpha_1 x_1 + \mathfrak{A}_1 x_1')^2 + (4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2)x_1'^2 + 2\alpha_1 \cdot f_2(x_\varrho) \pmod{2^{\iota+1}}$$

ist. Aus diesen Congruenzen folgen, wie in nr. 4, die Beziehungen

$$\omega_m(f^{(2)}) = \omega_m(f_2),\ \sigma_m(f^{(2)}) = \sigma_m(f_2)$$
$$(m = 1, 2, 3, \cdots n-3)$$

ferner

$$f^{(2)}(h, 2^t) = f_2(h, 2^t)$$

sowie die Congruenz

$$\Delta(f^{(2)}) \equiv \Delta(f_2) \pmod{2^{t+1}}$$

und folglich

$$f^{(2)} \simeq f_2 \pmod{2^t}.$$

Somit kann man durch eine nur die letzten $n-2$ Veränderlichen berührende unimodulare Substitution $f^{(2)}(x_\varrho)$ in eine Form $f''(x_\varrho)$ transformiren, welche denselben Rest (mod. 2^t) giebt wie $f_2(x_\varrho)$, und folglich wird die frühere Substitution, mit der letzteren zusammengesetzt, eine solche sein, deren Modulus gleich 1 also auch $\equiv 1$ (mod. 2^t) ist, deren erste Vertikalreihe die Zahlen $t_{11}, t_{21}, \cdots t_{n1}$ sind und welche den Rest von $f(x_\varrho)$ nicht verändert. Jeder Wurzel der Congruenz (62) entspricht also eine solche Substitution T.

Ist aber T eine solche, so wird auch jede Substitution $\mathrm{T} \cdot U$ eine solche sein, wenn U gleichfalls die Determinante $\equiv 1$ (mod. 2^t) hat und f (mod. 2^t) nicht verändert.

Damit letzteres der Fall sei, muss wegen (61) die Congruenz erfüllt sein:

$$2\alpha_1 U_1 + \mathfrak{A}_1 \cdot u_{11} \equiv \mathfrak{A}_1 \pmod{2^t} \tag{64}$$

und

$$f(U_1, u_{11}, \cdots u_{n-1,1}) \equiv 2\mathfrak{a}_1 \pmod{2^t}$$

oder

$$(2\alpha_1 U_1 + \mathfrak{A}_1 u_{11})^2 + (4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2)u_{11}^2 + 2\alpha_1 f_2(u_{21}, \cdots u_{n-1,1}) \equiv 4\alpha_1\mathfrak{a}_1 \pmod{2^{t+1}}$$

d. i. mit Beachtung von (64)

$$(4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2)\cdot u_{11}^2 + 2\alpha_1 f_2(u_{21}, \cdots u_{n-1,1}) \equiv 4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2 \pmod{2^{t+1}}. \tag{65}$$

Analoge Betrachtungen wie in nr. 4 und wie wir sie im Falle $\sigma_1 = 1$ angestellt haben, die jedoch einer Erweiterung der nur für ungerade Determinanten giltigen Grundlage bedürfen, lassen erkennen, dass jedem Systeme von Zahlen $u_{11}, u_{21}, \cdots u_{n-1,1}$ (mod. 2^t), welches dieser Congruenz

genügt, in der That eine Substitution U der gedachten Art zugehörig ist. Weil aber (s. siebentes Capitel nr. 1, 2) Anfang) immer 2^{n-1} Wurzeln dieser Congruenz (mod. 2^{t+1}) ein einziges (mod. 2^t) bestimmtes System solcher Zahlen entspricht, wird die Anzahl solcher Systeme $\frac{A'}{2^{n-1}}$ sein, wenn A' die gesammte Anzahl jener Wurzeln bezeichnet. Aus einer Substitution U der gedachten Art erhalten wir aber die anderen, demselben Systeme $u_{11}, u_{21}, \cdots u_{n-1,1}$ entsprechenden vermittelst der Formel $U \cdot V$, wenn darin unter V eine Substitution

$$V = \begin{pmatrix} 1 & U & V_2 & \cdots & V_n \\ 0 & 1 & V_2' & \cdots & V_n' \\ 0 & 0 & v_{11} & \cdots & v_{1,n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & v_{n-2,1} & \cdots & v_{n-2,n-2} \end{pmatrix}$$

verstanden wird, in der die Determinante

$$| v_{ix} | \equiv 1 \pmod{2^t}$$

ist und welche f (mod. 2^t) nicht verändert. Hierzu wird, wie leicht aus (61) erkennbar ist, erfordert, dass

$$\left.\begin{array}{l} 2\alpha_1 U + \mathfrak{A}_1 \equiv \mathfrak{A}_1, \ 2\alpha_1 V_h + \mathfrak{A}_1 V_h' \equiv 0 \\ 2\alpha_1 U^2 + 2\mathfrak{A}_1 U + 2\mathfrak{a}_1 \equiv 2\mathfrak{a}_1, \\ 2\alpha_1 U V_h + \mathfrak{A}_1 (V_h' U + V_h) + 2\mathfrak{a}_1 V_h' \equiv 0 \end{array}\right\} \pmod{2^t}$$

d. h.

$$2U \equiv 0, \ V_h \equiv 0, \ V_h' \equiv 0 \pmod{2^t}$$

mithin entweder $U \equiv 0$ oder $U \equiv 2^{t-1}$ (mod. 2^t) sei, und dass die Substitution (v_{ix}) die Form $f_2(x_\varrho)$ (mod. 2^t) nicht verändere. Jeder Substitution U der gedachten Art entsprechen daher $2 \cdot f_2(2^t)$ Substitutionen V von der verlangten Beschaffenheit.

Aus alle diesem erschliesst man, wenn A die Anzahl der Wurzeln der Congruenz (62), A' die Anzahl der Wurzeln der Congruenz (65) bezeichnet, die Recursionsformel

$$(66) \qquad f(2^t) = 2A \cdot \frac{A'}{2^{n-1}} \cdot f_2(2^t).$$

Wäre $n = 2$, so würde $f_2(x_\varrho)$ eine Form mit Null Veränderlichen; in diesem Falle aber sieht man leicht, dass, damit

$U = \begin{pmatrix} 1, & U \\ 0, & u_{11} \end{pmatrix}$ eine der bezeichneten Substitutionen sei, die Congruenzen

$$u_{11} \equiv 1,\ 2U \equiv 0 \pmod{2^t}$$

nothwendig und hinreichend sind; es giebt also **zwei** solche U und demnach entsprechen jeder Wurzel der Congruenz (62) zwei Substitutionen T, sodass dann

$$f(2^t) = 2A \tag{66a}$$

gefunden wird. Da man in demselben Falle $A' = 4$ findet, bleibt die allgemeine Formel (66) auch in ihm giltig, vorausgesetzt, dass man dann den Faktor $f_2(2^t)$ durch $\frac{1}{2}$ ersetzt. —

Da aber die Congruenz (62) keine Wurzeln in lauter geraden Zahlen gestattet, besitzt sie auch keine solchen, für welche sämmtliche Ausdrücke

$$\frac{1}{2}\,\frac{\partial f(x_\varrho)}{\partial x_i} \ (\text{für } i = 1, 2, \cdots n)$$

gerade sind. Nach nr. 1, 3) des vorigen Capitels findet man demnach zunächst

$$A = 2\mathsf{A} \cdot 2^{(n-1)(t-1)},$$

unter $2\mathsf{A} \cdot 2^{n-1}$ die Anzahl der Wurzeln verstanden, welche die Congruenz

$$f(x_\varrho) \equiv 2\alpha_1 \pmod{4} \tag{67}$$

erfüllen, und nach Formel (60) daselbst hat man

$$\mathsf{A} = 2^{n-1}\left(1 - \left(\frac{2}{\varDelta}\right)2^{-\frac{n}{2}}\right).$$

Die Anzahl A' der Wurzeln von (65) ist nach nr. 1, 2) des vorigen Capitels

$$A' = 2^{(n-2)(t-2)} \cdot \mathsf{A}',$$

wenn A' die Anzahl der Wurzeln der Congruenz

$$(4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2)x_1^2 + 2\alpha_1 \cdot f_2(x_2, \cdots x_{n-1}) \equiv 4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2 \pmod{8}$$

bezeichnet. Diese Congruenz erfordert x_1 als ungerade Zahl also (mod. 8) congruent mit einem der vier Werthe 1, 3, 5, 7; alsdann müssen $x_2, \cdots x_{n-1}$ der Congruenz

$$f_2(x_2, \cdots x_{n-1}) \equiv 0 \pmod{4}$$

Genüge leisten, welche, wenn unter Δ_1 die Determinante von f_2 verstanden wird, nach nr. 5 daselbst

$$2^{2n-5}\cdot\left(1+\left(\frac{2}{\Delta_1}\right)\cdot 2^{-\frac{n}{2}+1}\right)$$

Wurzeln (mod. 4) hat, mithin findet sich

$$A' = 2^{3n-5}\cdot\left(1+\left(\frac{2}{\Delta_1}\right)\cdot 2^{-\frac{n}{2}+1}\right)$$

also

$$\frac{A'}{2^{n-1}} = 2^{(n-2)t}\cdot\left(1+\left(\frac{2}{\Delta_1}\right)2^{-\frac{n}{2}+1}\right).$$

Durch alles dies gewinnt man endlich die Recursionsformel (66) in folgender Gestalt:

$$f(2^t) = 4\cdot 2^{(n-1)t+(n-2)t}\cdot\left(1-\left(\frac{2}{\Delta}\right)2^{-\frac{n}{2}}\right)$$
$$\cdot\left(1+\left(\frac{2}{\Delta_1}\right)2^{-\frac{n}{2}+1}\right)\cdot f_2(2^t).$$

Da für $t \gtreqless 3$

$$\Delta \equiv (4\alpha_1 \mathfrak{a}_1 - \mathfrak{A}_1^2)\cdot\Delta_1 \pmod{8},$$

so ist

$$\left(\frac{2}{\Delta_1}\right) = \left(\frac{2}{\Delta}\right)\cdot\left(\frac{2}{4\alpha_1\mathfrak{a}_1 - \mathfrak{A}_1^2}\right).$$

In derselben Weise aber findet sich

$$f_2(2^t) = 4\cdot 2^{(n-3)t+(n-4)t}\cdot\left(1-\left(\frac{2}{\Delta_1}\right)2^{-\frac{n}{2}+1}\right)$$
$$\cdot\left(1+\left(\frac{2}{\Delta_2}\right)2^{-\frac{n}{2}+2}\right)\cdot f_4(2^t)$$

worin

$$\left(\frac{2}{\Delta_2}\right) = \left(\frac{2}{\Delta_1}\right)\cdot\left(\frac{2}{4\alpha_2\mathfrak{a}_2 - \mathfrak{A}_2^2}\right)$$

zu setzen ist, u. s. w., zuletzt nach (66a)

$$f_{n-2}(2^t) = 4\cdot 2^t\left(1-\left(\frac{2}{\Delta_{\frac{n}{2}-1}}\right)2^{-1}\right),$$

und durch Multiplikation der so entstehenden Gleichungen ergiebt sich zuletzt

$$f(2^t) = 2^{\frac{n(n-1)}{2}t}\cdot\sigma_1\sigma_2\cdots\sigma_{n-1}\cdot f[2], \tag{68}$$

wenn zur Abkürzung

$$(69)\ f[2] = 2^{\frac{n}{2}} \cdot \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{2^4}\right) \cdots \left(1 - \frac{1}{2^n}\right) \cdot \left(1 + \left(\frac{2}{\varDelta}\right)\frac{1}{2^{\frac{n}{2}}}\right)^{-1}$$

gesetzt wird. —

11. Bevor wir dieses Capitel beschliessen, sei bemerkt, dass die Definition des Geschlechts noch auf eine neue Art gefasst werden kann. Es lässt sich nämlich, wie Minkowski anmerkt*), der Satz, den wir im ersten Abschnitte Seite 127 nach Smith ausgesprochen und bewiesen haben, auf Formen mit beliebig viel Veränderlichen ausdehnen, und man darf demgemäss sagen:

Zwei Formen eines Geschlechts lassen sich immer durch eine rationale Transformation, d. i. eine solche mit rationalen Coefficienten, mit dem Modulus 1 und mit einem zu einer beliebig gegebenen Zahl primen Generalnenner in einander transformiren und sind umgekehrt durch diese Eigenschaft als Formen eines Geschlechts charakterisirt.

Auf Grund dieses Satzes und indem er noch den im zweiten Abschnitte Seite 369 bewiesenen Satz über reducirte Substitutionen zu Hilfe nimmt, hat Minkowski in einer leider nur skizzirten Arbeit**) die Bedingungen untersucht, unter welchen zwei quadratische Formen mit rationalen Coefficienten rational in einander transformirt werden können. Ohne dass wir näher hier auf diese Untersuchung eingehen können, sollen doch ihre Hauptresultate der Vollständigkeit wegen noch angefügt werden.

Man darf die Betrachtung auf Formen mit ganzzahligen Coefficienten beschränken, denn jeder Form f mit rationalen Coefficienten kann, wenn N der Generalnenner ihrer Coefficienten ist, die ganzzahlige Form $N^2 \cdot f$ zugeordnet werden, in welche f durch die rationale Transformation

$$x_i = N \cdot x_i'$$

übergeht. Kann also f in f' rational transformirt werden,

---

*) Minkowski, über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Coefficienten in einander rational transformirt werden können, Journ. f. Math. 106.

**) Ebendaselbst.

welcher die Form $N'^2 \cdot f'$ zugeordnet ist, so kann es auch $N^2 \cdot f$ in $N'^2 \cdot f'$ und umgekehrt.

Eine ganzzahlige quadratische Form f mit n Veränderlichen und nicht verschwindender Determinante geht nun aber offenbar durch eine rationale Transformation mit nicht verschwindendem Modulus in eine andere über, bei welcher — ausser der Zahl n und dem Trägheitsindex τ — die Gesammtheit derjenigen Primzahlen ungeändert ist, welche in der Determinante in ungeraden Potenzen aufgehen. Setzt man deren Produkt, mit $(-1)^\tau$ multiplicirt, gleich A, so sind also n, τ, A arithmetische Invarianten mit Bezug auf alle jene Transformationen. Ausserdem giebt es aber, bezüglich auf jede ungerade Primzahl p, eine gewisse Einheit C_p und bezüglich des Modulus 4 oder 8 eine gewisse Einheit C_2, welche bei allen jenen Transformationen ungeändert bleiben; für alle nicht in der Determinante aufgehenden Primzahlen p ist stets $C_p = 1$. Man nenne B das Produkt aller ungeraden Primzahlen, für welche $C_p = -1$ ist, B das Produkt derjenigen von ihnen, die nicht in A enthalten sind. Auch diese Zahlen B, B sind mithin Invarianten, bleiben nämlich bei allen jenen Transformationen ungeändert. Dann gilt folgender Hauptsatz:

Zwei Formen mit n Veränderlichen und nicht verschwindenden Determinanten können dann und nur dann rational in einander transformirt werden, wenn sie gleiche Invarianten τ, A, B haben.

Man beachte ferner, dass beim Uebergange von f zu $M \cdot f$ der von quadratischen Faktoren befreite Kern der Determinante ungeändert gleich A bleibt, falls n gerade ist. Alsdann zeigt die nähere Untersuchung, dass eine Einheit C_p dann und nur dann für alle Vielfachen $M \cdot f$ gleichen Werth hat, wenn p in A nicht aufgeht und $(-1)^{\frac{n}{2}} \cdot A$ quadratischer Rest von p resp., für $p = 2$, von 8 ist. B_1 heisse das Produkt derjenigen unter diesen Primzahlen, für welche $C_p = -1$ ist; mithin ist die Zahl B_1 ein Theiler von B; sie kann als Invariante der Gleichung $f = 0$ bei rationalen Transformationen bezeichnet werden. Setzen wir

$$D = A \cdot \mathsf{B}_1^2,$$

wenn n gerade ist, so ist aus dem Werthe der einzigen Zahl D sowohl A als B_1 zu entnehmen, da A wie B_1 aus lauter verschiedenen Primfaktoren zusammengesetzt und prim gegen einander sind.

Ist n ungerade, so giebt es unter allen Vielfachen $M \cdot f$ ein einziges, nämlich $A \cdot f$, dessen Determinantenkern gleich 1 ist; die diesem Vielfachen entsprechende B-Invariante kann als die Invariante der Gleichung $f = 0$ bei rationalen Transformationen bezeichnet werden, und wir setzen für ungerade n

$$D = \text{dieser } B\text{-Invariante.}$$

Dann folgt aus dem Hauptsatze folgender andere:

Wenn zwei Formen mit n Veränderlichen und nicht verschwindender Determinante in den absoluten Werthen ihrer Zahlen $n - 2\tau$ und in ihren Invarianten D übereinstimmen, so kann jede von ihnen rational in ein rationales Vielfache der anderen transformirt werden.

Unter den besonderen Folgerungen aus diesen allgemeinen Sätzen, welche Minkowski zieht, seien nur die folgenden zwei erwähnt:

1) Von Null verschiedene rationale Quadratzahlen sind darstellbar durch jede nicht wesentlich negative quadratische Form mit 4 oder mehr Veränderlichen, durch jede solche Form mit 3 Veränderlichen, deren Invarianten A, B auch bei Formen mit 2 Veränderlichen vorkommen können, und durch jede solche Form mit 2 Veränderlichen, deren Invarianten A, B auch bei einer Form mit einer Veränderlichen vorkommen können.

2) Die Zahl Null ist rational darstellbar durch

jede unbestimmte quadratische Form mit 5 oder mehr Veränderlichen;

durch jede solche Form mit 4 Veränderlichen, deren Invariante D nur erste Primzahlpotenzen enthält;

durch jede solche Form mit 3 Veränderlichen, deren Invariante D gleich 1 ist;

durch jede solche Form mit 2 Veränderlichen, deren Invariante D gleich -1 ist.

Neuntes Capitel.

Die Darstellung durch eine quadratische Form.

1. Wir wenden uns nunmehr zu einer anderen Betrachtungsreihe. Schon bei den ternären Formen haben wir zu bemerken gehabt, dass dort neben der Aufgabe: eine gegebene Zahl durch eine solche Form darzustellen — eine Aufgabe, die bei den binären Formen die einzige dieser Art ausmacht — noch die andere auftrat: eine binäre Form durch eine ternäre Form darzustellen. Noch mannigfaltiger ist die Darstellungstheorie im Falle der Formen mit n Veränderlichen. Geht die quadratische Form

$$(1)\qquad f(x_\varrho)=\sum_{(\alpha,\beta=1,2,\cdots n)} a_{\alpha\beta}\, x_\alpha\, x_\beta$$

durch die Substitution

$$(2)\qquad x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho n} y_n \quad (\varrho = 1, 2, \cdots n)$$

in die Form

$$(3)\qquad g(y_\varrho)=\sum_{(\alpha,\beta=1,2,\cdots n)} b_{\alpha\beta}\, y_\alpha\, y_\beta$$

über, so wird, indem man $y_{\nu+1}, y_{\nu+2}, \cdots y_n$ gleich Null setzt, die Form

$$(4)\qquad \gamma(y_\varrho)=\sum_{(\alpha,\beta=1,2,\cdots \nu)} b_{\alpha\beta}\, y_\alpha\, y_\beta$$

von ν Veränderlichen $y_1, y_2, \cdots y_\nu$, welche ein Bestandtheil von $g(y_\varrho)$ ist, mittels der Formeln

$$(5)\qquad x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho \nu} y_\nu \quad (\varrho = 1, 2, \cdots n)$$

durch die Form $f(x_\varrho)$ dargestellt. Indem man

$$\nu = 1, 2, 3, \cdots n-1$$

setzt, erhält man somit die Darstellung einer Form mit einer Veränderlichen — oder, indem man für letztere den Werth 1 wählt, die Darstellung einer Zahl — dann einer Form mit $2, 3, \cdots n-1$ Veränderlichen durch die Form $f(x_\varrho)$, also neben den beiden, bei ternären Formen allein vorhandenen

Grenzfällen eine mit der Anzahl der Veränderlichen steigende Menge besonderer Fälle. Wir behandeln zunächst den allgemeinen Fall: die Darstellung einer Form mit $\nu < n$ Veränderlichen durch die Form $f(x_\varrho)$ mit n Veränderlichen.

1) Es bezeichne (5) irgend eine Darstellung der Form $\gamma(y_\varrho)$ durch die Form $f(x_\varrho)$. Die $n \cdot \nu$ Coefficienten in den darstellenden Formeln geben Entstehung zu den Determinanten ν^{ten} Grades

$$Q^{(\nu)}_{hik\cdots, 12\cdots\nu}, \tag{6}$$

in denen $hik\cdots$ irgend eine Combination von ν Zahlen der Reihe $1, 2, 3, \cdots n$ ist.

Wir nennen die Darstellung eine eigentliche, wenn diese Determinanten ohne gemeinsamen Theiler sind.

Setzen wir die Darstellung (5) als eine eigentliche voraus, so kann man nach nr. 5 des dritten Capitels eine Determinante $Q = |q_{i\varkappa}| = 1$ von $n \cdot n$ Elementen bilden, deren erste ν Spalten die Coefficienten von (5) sind, und ihnen entsprechend die unimodulare Substitution (2). Verwandelt letztere die Form $f(x_\varrho)$ in die äquivalente Form $g(y_\varrho)$, so bildet offenbar $\gamma(y_\varrho)$ denjenigen Bestandtheil der letzteren, welcher nur die Variabeln $y_1, y_2, \cdots y_\nu$ enthält. Lässt sich also $\gamma(y_\varrho)$ eigentlich durch $f(x_\varrho)$ darstellen, so giebt es eine mit $f(x_\varrho)$ äquivalente Form $g(y_\varrho)$, von welcher $\gamma(y_\varrho)$ ein Bestandtheil ist. — Ist umgekehrt $g(y_\varrho)$ irgend eine mit $f(x_\varrho)$ äquivalente Form, von welcher $\gamma(y_\varrho)$ der nur die Variabeln

$$y_1, y_2, \cdots y_\nu$$

enthaltende Bestandtheil ist, so liefert jede Substitution (2), durch welche $g(y_\varrho)$ aus $f(x_\varrho)$ hervorgeht, mittels der Formeln (5) eine Darstellung von $\gamma(y_\varrho)$ durch letztere Form und zwar eine eigentliche, weil die Zahlen (6), aus welchen die Determinante Q homogen und linear zusammengesetzt ist, wegen $Q = 1$ keinen gemeinsamen Theiler haben können.

Hieraus folgt sogleich, dass äquivalente Formen mit n Veränderlichen stets dieselben Formen mit ν Veränderlichen eigentlich darstellen. Denn, kann

$\gamma(y_\varrho)$ eigentlich durch $f(x_\varrho)$ dargestellt werden, so ist $f(x_\varrho)$ einer Form $g(y_\varrho)$ äquivalent, von welcher $\gamma(y_\varrho)$ derjenige Bestandtheil ist, welcher nur die Variabeln $y_1, y_2, \cdots y_\nu$ enthält. Ist nun $f(x_\varrho)$ äquivalent mit $f'(x_\varrho)$, so ist es auch $g(y_\varrho)$, und folglich kann, der letzten Bemerkung zufolge, $\gamma(y_\varrho)$ auch durch $f'(x_\varrho)$ eigentlich dargestellt werden.

2) Ferner sind offenbar zwei äquivalente Formen $\gamma(y_\varrho)$ und $\gamma'(z_\varrho)$ von ν Veränderlichen durch $f(x_\varrho)$ stets gleichzeitig eigentlich darstellbar resp. nicht darstellbar. Denn, wird mittels der Formeln

(5) $$x_\varrho = q_{\varrho 1}y_1 + q_{\varrho 2}y_2 + \cdots + q_{\varrho\nu}y_\nu$$
$$(\varrho = 1, 2, \cdots n)$$

$f(x_\varrho) = \gamma(y_\varrho)$, und mittels der unimodularen Substitution

(7) $$y_\varrho = \varkappa_{\varrho 1}z_1 + \varkappa_{\varrho 2}z_2 + \cdots + \varkappa_{\varrho\nu}z_\nu$$
$$(\varrho = 1, 2, \cdots \nu)$$

$\gamma(y_\varrho) = \gamma'(z_\varrho)$, so ist auch

$$f(x_\varrho) = \gamma'(z_\varrho)$$

mittels der Formeln

(8) $$x_\varrho = q'_{\varrho 1}z_1 + q'_{\varrho 2}z_2 + \cdots + q'_{\varrho\nu}z_\nu,$$
$$(\varrho = 1, 2, \cdots n)$$

wenn man setzt:

(9) $$q'_{\varrho\sigma} = q_{\varrho 1}\varkappa_{1\sigma} + q_{\varrho 2}\varkappa_{2\sigma} + \cdots + q_{\varrho\nu}\varkappa_{\nu\sigma}.$$
$$(\varrho = 1, 2, \cdots n;\ \sigma = 1, 2, \cdots \nu)$$

Giebt man in dieser Formel dem Index ϱ irgend welche ν Werthe $h, i, k, \cdots$ der Reihe $1, 2, \cdots n$, lässt aber σ alle seine Werthe durchlaufen, so erhält man $\nu \cdot \nu$ Elemente $q'_{\varrho\sigma}$, deren Determinante $Q'^{(\nu)}_{hik\cdots,12\cdots\nu}$ heisse; nach dem Multiplikationssatze für Determinanten ergiebt sich, da $|\varkappa_{\varrho\sigma}| = 1$ ist,

(10) $$Q'^{(\nu)}_{hik\cdots,12\cdots\nu} = Q^{(\nu)}_{hik\cdots,12\cdots\nu},$$

eine Gleichung, welche lehrt, dass die Darstellung von $\gamma'(z_\varrho)$ durch $f(x_\varrho)$ mit der Darstellung von $\gamma(y_\varrho)$ gleichzeitig eine eigentliche resp. nicht eigentliche ist.

3) Die eigentliche Darstellung (8) der Form $\gamma'(z_\varrho)$ soll der eigentlichen Darstellung (5) der Form $\gamma(y_\varrho)$ durch $f(x_\varrho)$ äquivalent genannt werden.

Es giebt so viel verschiedene, einer eigentlichen

Darstellung von $\gamma(y_\varrho)$ äquivalente Darstellungen von $\gamma'(z_\varrho)$, als es Transformationen jener Form in diese, oder Transformationen von $\gamma(y_\varrho)$ in sich selbst giebt. Da nämlich jede Transformation (7) der Form $\gamma(y_\varrho)$ in $\gamma'(z_\varrho)$ eine mit (5) äquivalente Darstellung (8) liefert, so ist zum Beweise der Aussage nur zu zeigen, dass verschiedenen Transformationen (7) auch verschiedene Darstellungen (8) entsprechen. Da aber die Darstellung (5) von $\gamma(y_\varrho)$ durch $f(x_\varrho)$ eine eigentliche sein soll, so können gewiss nicht sämmtliche Zahlen (6) Null sein; sei also etwa $Q^{(\nu)}_{hik\cdots,12\cdots\nu}$ von Null verschieden; dann bestimmen sich aus den ν Gleichungen (9), welche $\varrho = h, i, k, \cdots$ entsprechen, die Coefficienten

$$\varkappa_{1\sigma}, \varkappa_{2\sigma}, \cdots \varkappa_{\nu\sigma}$$

für jeden Werth von σ in eindeutiger Weise durch die Coefficienten $q'_{\varrho\sigma}$ und daher können nicht zwei verschiedene Transformationen (7) die gleiche Darstellung (8) hervorbringen.

4) Man überzeugt sich ferner leicht, dass die Bedingungen (10), welchen zwei äquivalente Darstellungen genügen, charakteristisch für sie sind, d. h. dass auch zwei Darstellungen äquivalent sein müssen, so oft sie ihnen genügen. Denn, da für die eigentliche Darstellung (5) die Zahlen $Q^{(\nu)}_{hik\cdots,12\cdots\nu}$ ohne gemeinsamen Theiler sind, kann man nach nr. 5 des dritten Capitels $n(n-\nu)$ Zahlen

$$q_{\varrho,\nu+1}, q_{\varrho,\nu+2}, \cdots q_{\varrho n}$$
$$(\varrho = 1, 2, \cdots n)$$

derart wählen, dass die Determinante $Q = | q_{i\varkappa} | = 1$ wird. Durch die Substitution

$$(11) \quad x_\varrho = q_{\varrho 1}y_1 + \cdots + q_{\varrho\nu}y_\nu + q_{\varrho,\nu+1}y_{\nu+1} + \cdots + q_{\varrho n}y_n$$
$$(\varrho = 1, 2, 3, \cdots n)$$

geht dann $f(x_\varrho)$ in eine äquivalente Form $g(y_\varrho)$ über, von welcher $\gamma(y_\varrho)$ derjenige Bestandtheil ist, der nur die Veränderlichen $y_1, y_2, \cdots y_\nu$ enthält. Erfüllt aber die Darstellung (8) die Bedingungen (10), so bilden auch die Gleichungen

$$(12) \quad x_\varrho = q'_{\varrho 1}z_1 + \cdots + q'_{\varrho\nu}z_\nu + q_{\varrho,\nu+1}z_{\nu+1} + \cdots + q_{\varrho n}z_n$$
$$(\varrho = 1, 2, 3, \cdots n)$$

eine unimodulare Substitution, durch welche $f(x_\varrho)$ in eine

äquivalente Form $g'(z_\varrho)$ übergeht; derjenige Bestandtheil der letzteren, welcher nur $z_1, z_2, \cdots z_\nu$ enthält, heisse $\gamma'(z_\varrho)$. Hiernach sind die Formen $g(y_\varrho)$ und $g'(z_\varrho)$ auch unter einander äquivalent und man erhält eine Transformation

$$y_\varrho = \varkappa_{\varrho 1} z_1 + \varkappa_{\varrho 2} z_2 + \cdots + \varkappa_{\varrho n} z_n \qquad (13)$$
$$(\varrho = 1, 2, \cdots n)$$

der ersten in die zweite, wenn man die Werthe (11) den Werthen (12) gleichsetzt und die so entstehenden Gleichungen:

$$q_{\varrho 1} y_1 + \cdots + q_{\varrho \nu} y_\nu + q_{\varrho, \nu+1} y_{\nu+1} + \cdots + q_{\varrho n} y_n$$
$$= q'_{\varrho 1} z_1 + \cdots + q'_{\varrho \nu} z_\nu + q_{\varrho, \nu+1} z_{\nu+1} + \cdots + q_{\varrho n} z_n$$
$$(\varrho = 1, 2, 3, \cdots n)$$

nach den y_i auflöst. Aus solcher Auflösung folgt offenbar

$$y_\varrho = \sum_{\sigma=1}^{\nu} (q'_{1\sigma} Q_{1\varrho} + q'_{2\sigma} Q_{2\varrho} + \cdots + q'_{n\sigma} Q_{n\varrho}) z_\sigma + \lambda_\varrho z_\varrho,$$

wo $\lambda_\varrho = 0$ ist für

$$\varrho = 1, 2, \cdots \nu,$$

und $\lambda_\varrho = 1$ für

$$\varrho = \nu + 1, \nu + 2, \cdots n.$$

Daher wird

$$\varkappa_{\varrho\sigma} = q'_{1\sigma} Q_{1\varrho} + q'_{2\sigma} Q_{2\varrho} + \cdots + q'_{n\sigma} Q_{n\varrho} \qquad (14)$$
$$(\varrho = 1, 2, \cdots n;\ \sigma = 1, 2, \cdots \nu)$$

dagegen für $\sigma > \nu$:

$$\left.\begin{matrix} \varkappa_{\varrho\sigma} = 1 \\ \varkappa_{\varrho\sigma} = 0 \end{matrix}\right\} \text{ jenachdem } \left\{\begin{matrix} \varrho = \sigma \\ \varrho \gtrless \sigma \end{matrix}\right. \text{ ist.}$$

Zudem ist, wenn $\varrho > \nu$ etwa $\varrho = \nu + h$ ist, der Ausdruck (14) für $\varkappa_{\varrho\sigma}$ nichts anderes als die Determinante Q, wenn in derselben die $\nu + h^{\text{te}}$ Spalte durch

$$q'_{1\sigma}, q'_{2\sigma}, \cdots q'_{n\sigma}$$

ersetzt wird. In der so entstehenden Determinante können jedoch wegen (10) die ersten ν Spalten durch die accentuirten Elemente ersetzt werden; da alsdann aber zwei Spalten derselben identisch werden, muss

$$\varkappa_{\varrho\sigma} = 0$$

sein, wenn

$$\varrho > \nu, \ \sigma = 1, 2, \cdots \nu$$

ist. Die Substitution (13) hat demnach die Form

$$\begin{aligned}
y_1 &= x_{11} z_1 + x_{12} z_2 + \cdots + x_{1\nu} z_\nu \\
&\cdots\cdots\cdots\cdots \\
y_\nu &= x_{\nu 1} z_1 + x_{\nu 2} z_2 + \cdots + x_{\nu\nu} z_\nu \\
y_{\nu+1} &= z_{\nu+1} \\
&\cdots\cdots \\
y_n &= z_n
\end{aligned}$$

und folglich verwandelt die unimodulare Substitution

$$y_\varrho = x_{\varrho 1} z_1 + x_{\varrho 2} z_2 + \cdots + x_{\varrho \nu} z_\nu \qquad (\varrho = 1, 2, \cdots \nu)$$

die Form $\gamma(y_\varrho)$ in $\gamma'(z_\varrho)$ und diese Formen sind äquivalent. Aus (14) endlich erhält man, wenn man σ festhält, dagegen ϱ alle Werthe $1, 2, 3, \cdots n$ durchlaufen lässt, n Gleichungen, aus denen sich

$$q'_{\varrho\sigma} = q_{\varrho 1} x_{1\sigma} + q_{\varrho 2} x_{2\sigma} + \cdots + q_{\varrho\nu} x_{\nu\sigma} \qquad (\varrho = 1, 2, \cdots n;\ \sigma = 1, 2, \cdots \nu)$$

findet. Diesen Beziehungen zufolge ist in der That die Darstellung (8) von $\gamma'(z_\varrho)$ der Darstellung (5) von $\gamma(y_\varrho)$ durch die Form $f(x_\varrho)$ äquivalent.

Da somit die Gleichungen (10) die nothwendige wie hinreichende Bedingung für die Aequivalenz zweier Darstellungen sind, sieht man sogleich ein, dass zwei Darstellungen, welche derselben dritten Darstellung äquivalent sind, es auch unter einander sind.

Identificirt man insbesondere die Formen $\gamma(y_\varrho)$, $\gamma'(z_\varrho)$, sodass die Substitution (7) eine Transformation von $\gamma(y_\varrho)$ in sich selbst darstellt, so lehren die entwickelten Sätze, dass sämmtliche eigentliche Darstellungen der Form $\gamma(y_\varrho)$ durch $f(x_\varrho)$ sich in eine Anzahl Complexe vertheilen lassen der Art, dass zwei Darstellungen äquivalent sind oder nicht, jenachdem sie demselben Complex angehören oder nicht, und dass in jedem Complexe sich so viel Darstellungen befinden, als es Transformationen von $\gamma(y_\varrho)$ in sich selbst giebt.

2. 1) Sei nun wieder (5) eine eigentliche Darstellung von $\gamma(y_\varrho)$ durch $f(x_\varrho)$ und (2) die entsprechende unimodulare Substitution. Weil $f(x_\varrho)$ durch letztere in $g(y_\varrho)$ übergeht, so

verwandelt sich nach nr. 7 des fünften Capitels die $n-1^{\text{te}}$ Begleitform

$$\sum A^{(n-1)}_{hik\cdots,\,rst\cdots}\cdot x_{hik\cdots}\cdot x_{rst\cdots}$$

von $f(x_\varrho)$ durch die Substitution

$$x_{hik\cdots}=\sum_{rst\cdots} Q^{(n-1)}_{hik\cdots,\,rst\cdots}\cdot y_{rst\cdots}$$

in die äquivalente Form

$$\sum B^{(n-1)}_{hik\cdots,\,rst\cdots}\cdot y_{hik\cdots}\cdot y_{rst\cdots}$$

d. i. in die $n-1^{\text{te}}$ Begleitform von $g(y_\varrho)$, oder, wenn man mit u, v diejenigen Indices der Reihe $1, 2, 3, \cdots n$ bezeichnet, welche resp. in der Combination der $n-1$ Indices $hik\cdots$, $rst\cdots$ fehlen, es verwandelt sich die Adjungirte von $f(x_\varrho)$:

$$F(x_\varrho)=\sum_{(u,\,v=1,\,2,\cdots n)} A_{uv}\cdot x_u x_v \tag{15}$$

durch die Substitution

$$x_\varrho = Q_{\varrho 1}y_1 + Q_{\varrho 2}y_2 + \cdots + Q_{\varrho n}y_n \qquad (\varrho=1,2,3,\cdots n) \tag{16}$$

in die Adjungirte

$$G(y_\varrho)=\sum_{(u,\,v=1,\,2,\cdots n)} B_{u,v}\cdot y_u y_v \tag{17}$$

von $g(y_\varrho)$. Demnach wird, wenn man $y_1, y_2, \cdots y_\nu$ gleich 0 setzt, die Form

$$\Gamma(y_\varrho)=\sum_{(u,\,v=\nu+1,\,\nu+2,\cdots n)} B_{uv}\, y_u y_v, \tag{18}$$

welche ein Bestandtheil von $G(y_\varrho)$ ist, mittels der Formeln

$$x_\varrho = Q_{\varrho,\nu+1}\cdot y_{\nu+1} + \cdots + Q_{\varrho,n}y_n \qquad (\varrho=1,2,3,\cdots n) \tag{19}$$

durch die Form $F(x_\varrho)$ dargestellt, und zwar eigentlich, da die aus den Coefficienten der Formeln (19) zu bildenden Determinanten

$$\mathfrak{Q}^{(n-\nu)}_{hi\varkappa\cdots;\,\nu+1,\,\nu+2,\cdots n} \tag{20}$$

vom Grade $n-\nu$, aus denen die Determinante $\mathfrak{Q}$ der Gleichungen (16) homogen und linear zusammengesetzt ist, wegen $\mathfrak{Q}=Q=1$ ohne gemeinsamen Theiler sind. Setzen wir an Stelle der A d j u n g i r t e n von $f(x_\varrho)$ und $g(y_\varrho)$ ihre p r i m i t i v e n

Adjungirten oder Reciproken

$$(21)\qquad \mathfrak{f}(x_\varrho) = \frac{(-1)^\tau \cdot F(x_\varrho)}{d_{n-2}} = \sum_{(u,v=1,2,\cdots n)} \mathfrak{a}_{uv}\, x_u\, x_v$$

$$(22)\qquad \mathfrak{g}(y_\varrho) = \frac{(-1)^\tau \cdot G(y_\varrho)}{d_{n-2}} = \sum_{(u,v=1,2,\cdots n)} \mathfrak{b}_{uv}\, y_u\, y_v$$

und

$$(23)\qquad \chi(y_\varrho) = \frac{(-1)^\tau \cdot \Gamma(y_\varrho)}{d_{n-2}} = \sum_{(u,v=\nu+1,\cdots n)} \mathfrak{b}_{uv}\, y_u\, y_v,$$

so wird offenbar mittels derselben Formel (19) $\chi(y_\varrho)$ durch die Form $\mathfrak{f}(x_\varrho)$ eigentlich dargestellt. Diese Darstellung (19) nennen wir der Darstellung (5) adjungirt. Aus der Reciprocität der beiden Formen $f(x_\varrho)$ und $\mathfrak{f}(x_\varrho)$ folgt dann ohne weiteres, dass auch umgekehrt der Darstellung (19) von $\chi(y_\varrho)$ durch $\mathfrak{f}(x_\varrho)$ die Darstellung (5) von $\gamma(y_\varrho)$ durch $f(x_\varrho)$ adjungirt ist. Hiernach gehören immer eine eigentliche Darstellung einer Form $\gamma(y_\varrho)$ mit ν Veränderlichen durch die Form $f(x_\varrho)$ und eine eigentliche — die adjungirte — Darstellung einer Form $\chi(y_\varrho)$ mit $n-\nu$ Veränderlichen durch die Reciproke von $f(x_\varrho)$ zu einander.

2) Nach den Formeln (12) und (15) des ersten Capitels besteht für zwei adjungirte Darstellungen (5) und (19) jede der Beziehungen:

$$(24)\qquad Q^{(\nu)}_{hik\cdots;\,12\cdots\nu} = \varepsilon \cdot \mathfrak{Q}^{(n-\nu)}_{h'i'\cdots;\,\nu+1,\cdots n}$$

wo $hik\cdots$ und $h'i'\cdots$ je zwei (geordnete) Combinationen von ν und $n-\nu$ Zahlen bezeichnen, die zusammengenommen die ganze Reihe $1, 2, 3, \cdots n$ erschöpfen, und

$$(24\text{a})\qquad \varepsilon = (-1)^{h+i+k+\cdots+1+2+\cdots+\nu}$$

zu setzen ist. Diese Beziehungen sind aber für zwei adjungirte Darstellungen charakteristisch, insofern zwei eigentliche Darstellungen (5) und (19), für welche sie stattfinden, auch immer adjungirte Darstellungen sind. Dies erkennt man folgendermassen. Sind die Coefficienten der eigentlichen Darstellungen (5) und (19) irgend welche Zahlen, welche die Bedingungen (24) erfüllen, so wähle

man $n \cdot \nu$ Zahlen

$$Q_{\varrho 1},\ Q_{\varrho 2},\ \cdots Q_{\varrho \nu} \qquad (\varrho = 1, 2, \cdots n)$$

so, dass die Determinante $\mathfrak{Q} = |\,Q_{i\varkappa}\,|$ gleich 1 wird, die Gleichungen

$$x_\varrho = Q_{\varrho 1} y_1 + \cdots + Q_{\varrho \nu} y_\nu + Q_{\varrho, \nu+1} y_{\nu+1} + \cdots + Q_{\varrho n} y_n \qquad (\varrho = 1, 2, 3, \cdots n)$$

also eine unimodulare Substitution bilden. Bezeichnen wir mit $\chi_{i\varkappa}$ das zu $Q_{i\varkappa}$ adjungirte Element der Determinante $\mathfrak{Q}$, so ist auch das System der Gleichungen

$$x_\varrho = \chi_{\varrho 1} y_1 + \cdots + \chi_{\varrho \nu} y_\nu + \chi_{\varrho, \nu+1} y_{\nu+1} + \cdots + \chi_{\varrho n} y_n \qquad (\varrho = 1, 2, 3, \cdots n)$$

eine unimodulare Substitution also ihre Determinante X gleich 1, und man hat die Beziehung

$$\mathsf{X}^{(\nu)}_{hik\cdots,\, 12\cdots\nu} = \varepsilon \cdot \mathfrak{Q}^{(n-\nu)}_{h'i'\cdots;\, \nu+1, \cdots n}, \tag{25}$$

in welcher $hik\cdots$, $h'i'\cdots$ wie in (24) und ε durch die Formel (24a) zu bestimmen sind. Da aber die Determinante X entsteht, wenn man die in vorstehender Gleichung auftretenden Unterdeterminanten mit anderen, nur die Elemente $\chi_{\varrho, \nu+1} \cdots \chi_{\varrho n}$ enthaltenden Unterdeterminanten multiplicirt, so wird ihr Werth, sobald die Gleichungen (24) erfüllt sind, ungeändert bleiben, wenn man die Zahlen $\chi_{\varrho 1}, \chi_{\varrho 2}, \cdots \chi_{\varrho \nu}$ durch $q_{\varrho 1}, q_{\varrho 2}, \cdots q_{\varrho \nu}$ ersetzt. Demnach wird auch

$$x_\varrho = q_{\varrho 1} y_1 + \cdots + q_{\varrho \nu} y_\nu + \chi_{\varrho, \nu+1} y_{\nu+1} + \cdots + \chi_{\varrho n} y_n \qquad (\varrho = 1, 2, 3, \cdots n)$$

eine unimodulare Substitution sein, in welcher die zu

$$\chi_{\varrho, \nu+1},\ \cdots \chi_{\varrho n}$$

adjungirten Elemente, wie man aus denselben Gründen wie bezüglich der Determinante X erkennt, die Zahlen

$$Q_{\varrho, \nu+1},\ \cdots Q_{\varrho n}$$

sein müssen. Die Darstellung (19) ist somit der Darstellung (5):

$$x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho \nu} y_\nu \qquad (\varrho = 1, 2, \cdots n)$$

in der That adjungirt.

3. Verbindet man diese Sätze über adjungirte Darstellungen nun mit denjenigen über äquivalente Darstellungen, so erkennt man sogleich die Richtigkeit des Satzes:

1) Zwei äquivalenten Darstellungen durch $f(x_\varrho)$ sind stets dieselben Darstellungen durch die Reciproke von $f(x_\varrho)$ adjungirt. Denn bezeichnet

$$x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho \nu} y_\nu \qquad (\varrho = 1, 2, \cdots n) \tag{26}$$

eine eigentliche Darstellung der Form $\gamma(y_\varrho)$ und

$$x_\varrho = q'_{\varrho 1} z_1 + q'_{\varrho 2} z_2 + \cdots + q'_{\varrho \nu} z_\nu \qquad (\varrho = 1, 2, \cdots n) \tag{27}$$

eine solche Darstellung der ihr äquivalenten Form $\gamma'(z_\varrho)$ durch $f(x_\varrho)$, welche der ersteren äquivalent ist, so bestehen die Beziehungen (10). Bedeutet ferner

$$x_\varrho = Q_{\varrho, \nu+1} y_{\nu+1} + \cdots + Q_{\varrho n} y_n \qquad (\varrho = 1, 2, \cdots n) \tag{28}$$

eine zur ersteren Darstellung adjungirte Darstellung durch die Reciproke von $f(x_\varrho)$, so bestehen die Beziehungen (24); und aus der Combination jener mit diesen erschliesst man die Gleichheiten

$$Q'^{(\nu)}_{hik \cdots ; 12 \cdots \nu} = \varepsilon \cdot \mathfrak{Q}^{(n-\nu)}_{h' i' \cdots ; \nu+1, \cdots n},$$

welche lehren, dass die Darstellung (28) auch der mit (26) äquivalenten Darstellung (27) adjungirt ist.

2) Man ersieht endlich auf diese Weise, dass ein- und dieselbe Darstellung durch die Reciproke von $f(x_\varrho)$ nur äquivalenten Darstellungen durch die Form $f(x_\varrho)$ selbst adjungirt sein kann.

4. Von dem bisher behandelten allgemeinen Falle der Darstellung einer Form mit ν Variabeln durch die Form

$$f(x_\varrho) = \sum a_{\alpha\beta} x_\alpha x_\beta \qquad (\alpha, \beta, = 1, 2, \cdots n)$$

resp. einer Form von $n - \nu$ Variabeln durch die Reciproke von $f(x_\varrho)$ gehen wir nun zu dem besonders wichtigen Grenzfalle über, in welchem $\nu = n - 1$ ist.

1) Eine quadratische Form

(29) $$b(y_\varrho) = \sum_{(\alpha,\beta, = 1, 2, \cdots n-1)} b_{\alpha\beta} y_\alpha y_\beta$$

ist eigentlich durch $f(x_\varrho)$ mittels der Formeln

(30) $$x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho, n-1} y_{n-1}$$
$$(\varrho = 1, 2, \cdots n)$$

darstellbar, wenn vermöge dieser Beziehungen

$$f(x_\varrho) = b(y_\varrho)$$

ist und die Zahlen

(31) $$Q^{(n-1)}_{hik\cdots;\,12\cdots n-1}$$

ohne gemeinsamen Theiler sind. Da alsdann eine unimodulare Substitution

(32) $$x_\varrho = q_{\varrho 1} y_1 + \cdots + q_{\varrho, n-1} y_{n-1} + q_{\varrho n} y_n$$
$$(\varrho = 1, 2, \cdots n)$$

angebbar ist, so verwandelt sich durch letztere $f(x_\varrho)$ in eine äquivalente Form

(33) $$g(y_\varrho) = \sum_{(\alpha,\beta, = 1, 2, \cdots n)} b_{\alpha\beta} y_\alpha y_\beta,$$

von welcher $b(y_\varrho)$ der von y_n freie Bestandtheil ist. Heisst $B_{i\varkappa}$ das zu $b_{i\varkappa}$ adjungirte Element der Determinante $B = |b_{i\varkappa}|$ der Form (33), so ist B_{nn} die Determinante von $b(y_\varrho)$. Nun ist aber $B_{nn} = (-1)^r d_{n-2} \cdot \mathfrak{b}_{nn}$ also theilbar durch d_{n-2}, und so gewinnt man das erste Ergebniss: **Durch die Form $f(x_\varrho)$ können nur solche Formen mit $n-1$ Veränderlichen eigentlich dargestellt werden, deren Determinante theilbar ist durch d_{n-2}.** Setzen wir demnach die Determinante von $b(y_\varrho)$ gleich $(-1)^r d_{n-2} \cdot b$, so wird $b = \mathfrak{b}_{nn}$.

2) **Ferner erschliesst man aus nr. 2, 1), dass jeder eigentlichen Darstellung** (20) **von** $b(y_\varrho)$ **durch** $f(x_\varrho)$ eine Darstellung der Form

$$\chi(y_\varrho) = \mathfrak{b}_{nn} \cdot y_n^2$$

durch die Reciproke von $f(x_\varrho)$ mittels der Formeln

$$x_1 = Q_{1n} y_n,\ x_2 = Q_{2n} y_n,\ \cdots x_n = Q_{nn} y_n$$

oder, was dasselbe sagt, **eine eigentliche Darstellung der** *Zahl* $\mathfrak{b}_{nn} = b$ **durch die Reciproke von** $f(x_\varrho)$ **mittels der** *Werthe*

$$x_1 = Q_{1n},\ x_2 = Q_{2n},\ \cdots x_n = Q_{nn}$$

adjungirt ist; sowie

3) dass auch umgekehrt jede eigentliche Darstellung der Zahl b durch die Reciproke von $f(x_\varrho)$ einer eigentlichen Darstellung einer Form mit $n-1$ Veränderlichen und der Determinante B_{nn} durch $f(x_\varrho)$ selbst adjungirt sein muss.

4) Nach nr. 3, 1) sind äquivalenten Darstellungen von Formen mit $n-1$ Veränderlichen und der Determinante B_{nn} durch die Form $f(x_\varrho)$ stets gleiche Darstellungen von b durch die Reciproke von $f(x_\varrho)$ adjungirt und

5) nach nr. 3, 2) müssen nicht-äquivalenten Darstellungen solcher Formen durch $f(x_\varrho)$ verschiedene Darstellungen von b durch die Reciproke von $f(x_\varrho)$ adjungirt sein.

Hieraus ergiebt sich folgende Regel, um sämmtliche verschiedene eigentliche Darstellungen der Zahl b durch die Reciproke von $f(x_\varrho)$ zu ermitteln:

Nach 3) werden sie sämmtlich gefunden, wenn man die eigentlichen Darstellungen (30) aller Formen mit $n-1$ Veränderlichen und der Determinante $(-1)^r d_{n-2} \cdot b$ durch $f(x_\varrho)$ aufsucht und vermittelst derselben die Zahlen

$$Q_{1n},\ Q_{2n},\ \cdots Q_{nn}$$

bestimmt. Nach 4) genügt es aber, nur nicht-äquivalente Darstellungen zu betrachten. Man wähle also von allen jenen Formen nur die Repräsentanten eines vollständigen Systems nicht-äquivalenter Formen, bilde für jeden von ihnen die Complexe äquivalenter Darstellungen, deren er fähig ist, und wähle aus jedem solchen Complexe nur eine einzige Darstellung. Nach 2) erhält man für jede solche Darstellung durch $f(x_\varrho)$ wirklich eine adjungirte Darstellung von b durch die Reciproke von $f(x_\varrho)$, und endlich werden alle diese Darstellungen von b nach 5) auch von einander verschieden sein.

Die Aufgabe, alle Darstellungen einer gegebenen *Zahl* durch eine gegebene Form mit n Veränderlichen zu finden, kömmt den erhaltenen Ergebnissen zufolge

auf die andere zurück: alle Darstellungen einer *Form mit* $n-1$ *Veränderlichen* durch eine Form der erstgenannten Art zu ermitteln.

5. Zur Lösung der letzteren Aufgabe suchen wir vor allem die Bedingungen auf, welche die Form (29) erfüllen muss, damit sie durch die Form

$$f(x_\varrho) = \sum_{(\alpha, \beta, = 1, 2, \cdots n)} a_{\alpha\beta} x_\alpha x_\beta$$

mit n Veränderlichen eigentlich darstellbar sei.

1) Wir wissen bereits, dass die Determinante B der Form $b(y_\varrho)$ durch d_{n-2} theilbar sein muss:

$$\mathsf{B} = (-1)^\tau d_{n-2} \cdot b. \tag{34}$$

Wenn dann $b(y_\varrho)$ durch $f(x_\varrho)$ mittels der Formeln (30) eigentlich darstellbar ist, so giebt es eine unimodulare Substitution (32), durch welche $f(x_\varrho)$ in die äquivalente Form (33) übergeht, deren Determinante B heisse. Die Reciproke von $f(x_\varrho)$:

$$\mathfrak{f}(x_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} \mathfrak{a}_{\alpha\beta} x_\alpha x_\beta$$

geht durch die Substitution

$$x_\varrho = Q_{\varrho 1} y_1 + Q_{\varrho 2} y_2 + \cdots + Q_{\varrho n} y_n \qquad (\varrho = 1, 2, \cdots n) \tag{35}$$

in die Reciproke von $g(y_\varrho)$:

$$\mathfrak{g}(y_\varrho) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} \mathfrak{b}_{\alpha\beta} y_\alpha y_\beta$$

über, und folglich besteht noch folgende allgemeine Beziehung:

$$\mathfrak{b}_{ix} = \sum_{u, v} \mathfrak{a}_{uv} \cdot Q_{ui} \cdot Q_{vx}. \tag{36}$$

Aus ihr findet sich insbesondere für $\mathfrak{b}_{nn} = b$ die Formel:

$$b = \mathfrak{f}(Q_{\varrho n}) \tag{37}$$

d. h. b ist eigentlich durch die Reciproke von $f(x_\varrho)$ also auch durch $\mathfrak{f}(x_\varrho)$ darstellbar, und somit muss

2) die Zahl b bezüglich jeder in o_{n-1} aber nicht in b aufgehenden ungeraden Primzahl p_{n-1} denselben quadratischen Charakter haben, wie die Zahl

$$\mathfrak{f}_1' = (-1)^{\tau} f_{n-1}',$$

was folgende Bedingung ergiebt:

$$(38) \qquad \left(\frac{b}{p_{n-1}}\right) = \left(\frac{\mathfrak{f}_1'}{p_{n-1}}\right) = \left(\frac{(-1)^{\tau} f_{n-1}'}{p_{n-1}}\right).$$

Weiter aber erschliesst man aus der Determinantenformel

$$B \cdot \frac{\partial^2 B}{\partial b_{nn} \partial b_{i\varkappa}} = B_{nn} \cdot B_{i\varkappa} - B_{n\varkappa} B_{in},$$

wenn man die Coefficienten

$$\mathfrak{b}_{i\varkappa} = (-1)^{\tau} \cdot \frac{B_{i\varkappa}}{d_{n-2}}$$

der Reciproken $\mathfrak{g}(y_\varrho)$ einführt und

$$(39) \qquad \frac{\partial^2 B}{\partial b_{nn} \partial b_{i\varkappa}} = \frac{\partial \mathsf{B}}{\partial b_{i\varkappa}} = d_{n-3} \cdot \beta_{i\varkappa}$$

setzt, was geschehen kann, da der Ausdruck als Unterdeterminante $n-2^{\text{ten}}$ Grades von B durch d_{n-3} aufgeht, die nachstehende Gleichung:

$$(-1)^{\tau} d_{n-1} d_{n-3} \cdot \beta_{i\varkappa} = d_{n-2}^2 (b\mathfrak{b}_{i\varkappa} - \mathfrak{b}_{in} \mathfrak{b}_{\varkappa n}).$$

Einfacher hat man

$$(40) \qquad (-1)^{\tau} o_{n-1} \cdot \beta_{i\varkappa} = b\mathfrak{b}_{i\varkappa} - \mathfrak{b}_{in} \mathfrak{b}_{\varkappa n}, \qquad (i, \varkappa = 1, 2, \cdots n-1)$$

Gleichungen, welche in der Form von Congruenzen auch so geschrieben werden können:

$$(41) \qquad (-1)^{\tau+1} o_{n-1} \cdot \beta_{i\varkappa} \equiv \mathfrak{b}_{in} \mathfrak{b}_{\varkappa n} \pmod{b} \qquad (i, \varkappa = 1, 2, \cdots n-1)$$

und sich in folgende eine Congruenz:

$$(42) \qquad \begin{cases} (-1)^{\tau+1} \cdot o_{n-1} \cdot \sum\limits_{(i, \varkappa = 1, 2, \cdots n-1)} \beta_{i\varkappa} y_i y_\varkappa \\ \equiv (\mathfrak{b}_{1n} y_1 + \mathfrak{b}_{2n} y_2 + \cdots + \mathfrak{b}_{n-1,n} y_{n-1})^2 \pmod{b} \end{cases}$$

zusammenfassen lassen. Letztere nimmt, wenn

$$(43) \qquad \beta(y_\varrho) = (-1)^{\tau} \cdot \sum_{(i, \varkappa = 1, 2, \cdots n-1)} \beta_{i\varkappa} y_i y_\varkappa = \sum_{(i, \varkappa = 1, 2, \cdots n-1)} \frac{(-1)^{\tau}}{d_{n-3}} \frac{\partial \mathsf{B}}{\partial b_{i\varkappa}} y_i y_\varkappa$$

gesetzt wird, diese Gestalt an:

$$(44) \qquad -o_{n-1} \cdot \beta(y_\varrho) \equiv (\mathfrak{b}_{1n} y_1 + \mathfrak{b}_{2n} y_2 + \cdots + \mathfrak{b}_{n-1,n} y_{n-1})^2 \pmod{b}.$$

3) Die eigentliche Darstellbarkeit der Form $b(y_\varrho)$ durch eine Form mit n Veränderlichen erfordert mithin die Möglichkeit dieser Congruenz d. h. das Vorhandensein von $n-1$ Zahlen

$$\mathfrak{b}_{1n},\ \mathfrak{b}_{2n},\ \cdots \mathfrak{b}_{n-1,n}, \tag{45}$$

welche derselben, oder, was dasselbe sagt, dem Systeme der Congruenzen (41) Genüge leisten; kurz gesagt:

$$-\,o_{n-1}\cdot\beta(y_\varrho)$$

muss ein quadratischer Rest (mod. b) sein.

6. Dem Bewiesenen zufolge entspricht jeder eigentlichen Darstellung (30) der Form $b(y_\varrho)$ mit $n-1$ Veränderlichen durch die Form $f(x_\varrho)$ mit n Veränderlichen ein System von $n-1$ Zahlen (45), welches der Congruenz (44) Genüge leistet. Ihre Werthe sind abhängig von der besonderen Wahl der Zahlen

$$q_{1n},\ q_{2n},\ \cdots q_{nn}, \tag{46}$$

welche mit der Darstellung (30) zusammen eine unimodulare Substitution (32) hervorbringen. Es lässt sich jedoch beweisen, dass die *Reste* der Zahlen (45) (mod. b) von dieser Wahl unabhängig sind. Zu diesem Zwecke entnehmen wir der Formel (36) die folgende:

$$\mathfrak{b}_{in}=\sum_{u,v}\mathfrak{a}_{uv}\,Q_{ui}\,Q_{vn}$$

und bilden, indem wir sie mit q_{ri} multipliciren, die nachstehende Summe:

$$\sum_{i=1}^{n} q_{ri}\,\mathfrak{b}_{in}=\sum_{u,v}\Big(\mathfrak{a}_{uv}\,Q_{vn}\cdot\sum_{i=1}^{n} q_{ri}\,Q_{ui}\Big);$$

den Beziehungen zwischen den Elementen q_{ix} und ihren adjungirten Elementen Q_{ix} zufolge ist

$$\sum_{i=1}^{n} q_{ri}\,Q_{ui}=1 \text{ oder } =0,$$

jenachdem $u=r$ oder $u\gtrless r$ ist, und somit nimmt die vorige Gleichung die einfachere Gestalt an:

$$\sum_{i=1}^{n} q_{ri}\,\mathfrak{b}_{in}=\sum_{v}\mathfrak{a}_{rv}\,Q_{vn},$$

wofür man schreiben kann:

$$(47)\qquad q_{r n}\cdot \mathfrak{b}_{n n} = \sum_{v}' \mathfrak{a}_{r v} Q_{v n} - \sum_{i=1}^{n-1}' q_{r i}\mathfrak{b}_{i n},$$

oder, da $\mathfrak{b}_{n n} = b$ ist, in Gestalt einer Congruenz:

$$(48)\qquad \sum_{v}' \mathfrak{a}_{r v} Q_{v n} \equiv \sum_{i=1}^{n-1}' q_{r i}\mathfrak{b}_{i n} \pmod{b}.$$
$$(r = 1, 2, \cdots n)$$

Ist nun $p^{\varkappa}$ irgend eine in b aufgehende Primzahlpotenz, so ergeben sich aus je $n-1$ dieser Congruenzen die Zahlen

$$Q_{1 n}\cdot \mathfrak{b}_{i n},\ Q_{2 n}\cdot \mathfrak{b}_{i n},\ \cdots Q_{n n}\cdot \mathfrak{b}_{i n}$$
$$(i = 1, 2, \cdots n-1)$$

unabhängig von der besonderen Wahl der Zahlen (46) (mod. $p^{\varkappa}$) bestimmt, und da die Zahlen $Q_{1 n}, Q_{2 n}, \cdots Q_{n n}$ nicht gleichzeitig durch p theilbar sein können, wird auch $\mathfrak{b}_{i n}$ d. i. jede der Zahlen (45) (mod. $p^{\varkappa}$) mithin auch (mod. b) vollkommen bestimmt sein. Verschiedenen Systemen (46) entsprechen daher (mod. b) congruente Systeme (45) oder ein- und dieselbe *Wurzel* der Congruenz (44).

Durch geeignete Wahl der Zahlen (46) kann man aber bewirken, dass die Zahlen (45) *irgend ein beliebiger Repräsentant* dieser Wurzel werden. Sind nämlich

$$(45')\qquad \mathfrak{b}'_{1 n}, \mathfrak{b}'_{2 n}, \cdots \mathfrak{b}'_{n-1, n}$$

irgend welche bestimmte Zahlen, welche (mod. b) den Zahlen (45) congruent sind, so dass allgemein

$$\mathfrak{b}'_{i n} = \mathfrak{b}_{i n} + b\cdot m_i = \mathfrak{b}_{i n} + \mathfrak{b}_{n n}\cdot m_i$$

gesetzt werden kann, so entspringen aus den Gleichungen (47) die ähnlichen:

$$q'_{r n}\mathfrak{b}_{n n} = \sum_{v}' \mathfrak{a}_{u v} Q_{v n} - \sum_{i=1}^{n-1}' q_{r i}\mathfrak{b}'_{i n},$$

wenn

$$q'_{r n} = q_{r n} - \sum_{i=1}^{n-1}' m_i q_{r i}$$

gesetzt wird. Die so bestimmten Zahlen $q'_{1 n}, q'_{2 n}, \cdots q'_{n n}$ sind aber auch ein zulässiges System von Zahlen (46), da, wenn

sie in der Determinante $|q_{i\varkappa}|$ statt dieser Zahlen gesetzt werden, der Werth derselben unverändert gleich 1 bleibt, und ihrer Wahl entspricht dann die Auflösung der Congruenz (44) mittels der Zahlen (45′).

Diese Ergebnisse lassen sich in dem Ausspruche zusammenfassen, dass jede mögliche eigentliche Darstellung der Form $b(y_\varrho)$ durch die Form $f(x_\varrho)$ zu einer ganz bestimmten *Wurzel* der Congruenz (44) führt oder — nach Gauss'scher Ausdrucksweise — gehört.

Aus dem zuletzt bewiesenen Punkte geht hervor, dass jeder eigentlichen Darstellung der Form $b(y_\varrho)$ durch die Form $f(x_\varrho)$, welche zu einer Wurzel der Congruenz (44) gehört, eine Transformation (32) von $f(x_\varrho)$ in eine, die Form $b(y_\varrho)$ als Bestandtheil enthaltende äquivalente Form $g(y_\varrho)$ entspricht, in deren Reciproken $\mathfrak{g}(y_\varrho)$ ein beliebig gewählter Repräsentant $\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$ jener Wurzel und die Zahl $\mathfrak{b}_{nn} = b$ die letzte Zeile (Spalte) des Coefficientensystems ausmachen. Jede mögliche eigentliche Darstellung von $b(y_\varrho)$ durch $f(x_\varrho)$, welche zu jener Wurzel gehört, muss hiernach erhalten werden, wenn man alle Transformationen von $f(x_\varrho)$ in diese Form $g(y_\varrho)$ aufsucht. Offenbar liefert aber auch jede solche Transformation eine jener Darstellungen, indem man in ihr die letzte Veränderliche zu Null macht. Und endlich werden verschiedenen solcher Transformationen auch verschiedene Darstellungen entsprechen; denn, bleibt die Darstellung (30) sowie auch der Repräsentant $\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$ der Wurzel der Congruenz (44) ungeändert, so bleiben es sämmtliche Zahlen zur Rechten der Gleichungen (47), und da auch $\mathfrak{b}_{nn} = b$ bleibt, können auch die Zahlen $q_{1n}, q_{2n}, \cdots q_{nn}$ und die Transformation (32) dann keine Veränderung erleiden.

7. Wir fahren zunächst noch in der Aufsuchung der Bedingungen fort, welche die Form $b(y_\varrho)$ erfüllen muss, um durch $f(x_\varrho)$ eigentlich darstellbar zu sein, und fragen deshalb nach dem Index, nach der Ordnung und nach dem Geschlechte, die $b(y_\varrho)$ hierfür zukommen müssen. Da jedenfalls b durch die Reciproke von $f(x_\varrho)$ eigentlich darstellbar sein muss, deren erste σ-Invariante gleich σ_{n-1} d. i. bei ungerader Deter-

minante gleich σ_1 ist, dürfen wir $b = \varepsilon\sigma_1 m$ setzen, wo $\varepsilon = \pm 1$, m aber positiv ist. Die Anwendungen, welche wir von der Theorie der Darstellung durch eine Form zu machen gedenken, gestatten uns, m als eine gegen 2Δ prime Zahl vorauszusetzen, und wir halten von nun an diese Voraussetzung fest. Ferner dürfen wir, da äquivalente Formen mit $n-1$ Veränderlichen stets gleichzeitig durch $f(x_\varrho)$ eigentlich darstellbar sind resp. nicht darstellbar, die Form $b(y_\varrho)$ ganz beliebig in ihrer Classe, z. B. als charakteristische Form derselben gewählt denken.

1) Wird dann unter B_m diejenige Unterdeterminante von $B = |b_{ix}|$ verstanden, die aus den ersten m Zeilen und Spalten gebildet ist, sodass

$$B_n = B = (-1)^\tau d_{n-1},\; B_{n-1} = B_{nn} = (-1)^\tau d_{n-2} b$$

also

$$B_{n-1} B_n = d_{n-1} d_{n-2} b$$

von demselben Vorzeichen ist wie b, so werden die Zahlen $B_1, B_2, \cdots B_{n-1}, B_n$ von Null verschieden sein. Demnach kann nach der Formel von Jacobi

$$g(y_\varrho) = \frac{Y_1^2}{B_1} + \frac{Y_2^2}{B_1 B_2} + \cdots + \frac{Y_{n-1}^2}{B_{n-2} B_{n-1}} + \frac{Y_n^2}{B_{n-1} B_n}$$

gesetzt werden. $Y_1, Y_2, \cdots Y_n$ bedeuten reelle lineare Funktionen von $y_1, y_2, \cdots y_n$. Die Anzahl der negativen Glieder zur Rechten ist der Trägheitsindex der Form $g(y_\varrho)$ also, da diese mit $f(x_\varrho)$ äquivalent ist, gleich τ. Aus gleichem Grunde lässt sich

$$b(y_\varrho) = \frac{Y_1'^2}{B_1} + \frac{Y_2'^2}{B_1 B_2} + \cdots + \frac{Y_{n-1}'^2}{B_{n-2} B_{n-1}}$$

setzen, wo jetzt $Y_1', Y_2', \cdots Y_{n-1}'$ reelle lineare Funktionen von $y_1, y_2, \cdots y_{n-1}$ bedeuten. Ist τ' der Trägheitsindex dieser Form $b(y_\varrho)$, d. i. die Anzahl der negativen Glieder zur Rechten, so ergiebt sich sogleich $\tau = \tau'$ oder $\tau = \tau' + 1$, jenachdem b positiv oder negativ ist. Soll also die Form $b(y_\varrho)$ durch $f(x_\varrho)$ eigentlich darstellbar sein, so muss ihr Trägheitsindex τ' gleich τ oder $\tau - 1$ sein, jenachdem b positiv oder negativ ist. — In dem besonderen Falle, in welchem $\tau = 0$ also $f(x_\varrho)$ eine positive Form ist, kann τ'

den zweiten Werth nicht haben, also hat τ' den Werth Null, b muss positiv und die Form $b(y_\varrho)$ eine positive Form sein.

2) Bei der Feststellung der Ordnung der Form $b(y_\varrho)$ halten wir die Voraussetzung fest, dass die Determinante Δ von $f(x_\varrho)$ ungerade sei. Mit d_0' werde der grösste gemeinsame Theiler aller Coefficienten von $b(y_\varrho)$, mit d_{h-1}' der grösste gemeinsame Theiler aller Unterdeterminanten h^{ten} Grades ihrer Determinante B, mit

$$\tau', \begin{matrix} o_1', o_2', \cdots o_{n-2}' \\ \sigma_1', \sigma_2', \cdots \sigma_{n-2}' \end{matrix}$$

die Ordnung der primitiven Form $\frac{b(y_\varrho)}{d_0'}$ bezeichnet. Dann besteht für den numerischen Werth d_{n-2}' der Determinante B die Gleichung

$$(49) \qquad d_{n-2}' = d_0'^{\,n-1} \cdot o_1'^{\,n-2}\, o_2'^{\,n-3} \cdots o_{n-3}'^{\,2}\, o_{n-2}' = \sigma_1\, d_{n-2}\, m,$$

aus welcher zunächst die Invarianten σ_i' leicht zu erschliessen sind.

Ist nämlich erstens $\sigma_1 = 1$, der ungeraden Determinante Δ wegen also auch $\sigma_2, \sigma_3, \cdots \sigma_{n-1}$ gleich 1, so ist nach der über m gemachten Annahme die Determinante der Form $\frac{b(y_\varrho)}{d_0'}$ ungerade, und folglich sind,

wenn n gerade also $n-1$ ungerade ist, nothwendig

$$\sigma_1' = 1,\ \sigma_2' = 1,\ \cdots \sigma_{n-2}' = 1$$

also

$$\sigma_1' = \sigma_1,\ \sigma_2' = \sigma_2,\ \cdots \sigma_{n-2}' = \sigma_{n-2};$$

wenn dagegen n ungerade also $n-1$ gerade ist, können auch

$$\sigma_1' = 2,\ \sigma_2' = 1,\ \sigma_3' = 2,\ \cdots \sigma_{n-2}' = 2$$

sein. — Ist dagegen zweitens $\sigma_1 = 2$ also der ungeraden Determinante Δ wegen n gerade und

$$\sigma_2 = 1,\ \sigma_3 = 2,\ \sigma_4 = 1,\ \cdots \sigma_{n-2} = 1,$$

so können durch $f(x_\varrho)$ und folglich auch, wenn $b(y_\varrho)$ durch $f(x_\varrho)$ darstellbar ist, durch $b(y_\varrho)$ nur gerade Zahlen dargestellt werden. Nun wird sogleich gezeigt werden, dass d_0' nicht gerade sein kann, also sind auch durch $\frac{b(y_\varrho)}{d_0'}$ nur gerade Zahlen

darstellbar und somit ist $\sigma_1' = 2$. Ferner folgt aus (49), wenn $2^{\omega_m'}$ die höchste in o_m' aufgehende Potenz von 2 bezeichnet, die Beziehung

$$(n-2)\omega_1' + (n-3)\omega_2' + \cdots + 2\omega_{n-3}' + \omega_{n-2}' = 1$$

d. h. die Werthe

$$\omega_1' = \omega_2' = \cdots = \omega_{n-3}' = 0, \ \omega_{n-2}' = 1;$$

sämmtliche Invarianten $o_1', o_2', \cdots o_{n-3}'$ also sind ungerade, o_{n-2}' das Doppelte einer ungeraden Zahl. Hieraus ergeben sich nach nr. 6 des sechsten Capitels sogleich folgende Werthe der Invarianten σ_i':

$$\sigma_1' = 2, \ \sigma_2' = 1, \cdots \sigma_{n-3}' = 2 \text{ und } \sigma_{n-2}' = 1$$

d. i.

$$\sigma_1' = \sigma_1, \ \sigma_2' = \sigma_2 \cdots \sigma_{n-3}' = \sigma_{n-3}, \ \sigma_{n-2}' = \sigma_{n-2}.$$

Wir haben noch zu zeigen, dass d_0' nicht gerade sein kann. Ginge aber 2 in d_0' also in sämmtlichen Coefficienten von $b(y_\varrho)$ auf, so wäre auch jede der Grössen

$$\frac{\partial \mathrm{B}}{\partial b_{i\varkappa}} = d_{n-3} \cdot \beta_{i\varkappa} \tag{50}$$

also, da d_{n-3} ungerade ist, jede der Grössen $\beta_{i\varkappa}$ durch 2 theilbar, ebenso wegen (49) die Zahl b, und somit folgte aus der Congruenz (44), dass auch jede der Zahlen

$$\mathfrak{b}_{1n}, \ \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$$

durch 2 theilbar wäre; mithin lieferten die Congruenzen (48) die folgenden:

$$\sum_v \mathfrak{a}_{rv} Q_{vn} \equiv 0 \pmod{2}, \quad (r = 1, 2, \cdots n)$$

welche unmöglich sind, denn die Determinante derselben ist, als Determinante der Reciproken $\mathfrak{f}(x_\varrho)$, ebenso ungerade, als der Voraussetzung nach die Determinante von $f(x_\varrho)$, die Grössen $Q_{1n}, Q_{2n}, \cdots Q_{nn}$ müssten also, obwohl sie keinen gemeinsamen Theiler haben können, gleichzeitig gerade sein.

Genau die gleichen Erwägungen führen zu dem Ergebnisse, dass weder d_0' noch eine der Invarianten $o_1', o_2', \cdots o_{n-3}'$ durch eine in m (also in b aber nicht in $\varDelta$) aufgehende Primzahl p theilbar sein kann. In der

That müsste solche Primzahl in allen Unterdeterminanten der Determinante B vom Grade $n-2$ und folglich auch in allen Zahlen (50) und, weil nicht in d_{n-3}, in allen Zahlen $\beta_{i\varkappa}$ aufgehen, was in Verbindung mit dem Umstande, dass die Determinante der Form $\mathfrak{f}(x_\varrho)$ ebenso wie Δ prim ist gegen m, auf gleiche Weise wie zuvor die Behauptung erweist.

Da dies für jede in m enthaltene Primzahl gilt, schliesst man aus der Gleichung (49), dass o'_{n-2} durch $\varepsilon\sigma_1 m = b$ theilbar sein muss.

Nun bedeute p irgend eine in d_{n-2} also nicht in $\sigma_1 m$ enthaltene Primzahl und p^{∂_m}, $p^{\partial'_m}$ die höchsten in d_m, d'_m resp. aufgehenden Potenzen derselben. Aus (49) ergiebt sich sogleich

$$\partial'_{n-2} = \partial_{n-2}.$$

Ferner muss unter den Unterdeterminanten m^{ten} Grades von B eine, und demnach auch diese eine unter den Unterdeterminanten m^{ten} Grades von B genau durch $p^{\partial'_{m-1}}$ aufgehen. Ihre Subdeterminanten sind durch

$$p^{\partial'_{m-2}} = p^{\partial_{m-2}+\delta}$$

theilbar, wo δ eine nicht-negative Zahl bezeichnet. Nach der Anmerkung auf S. 316 geht daher die Unterdeterminante selber durch $p^{\partial_{m-1}+\delta}$ auf, mithin muss

$$\partial'_{m-1} \geqq \partial_{m-1} + \delta$$

sein. Hat man folglich bewiesen, dass $\partial'_{m-1} = \partial_{m-1}$ ist, so muss $\delta = 0$ und folglich auch $\partial'_{m-2} = \partial_{m-2}$ sein. Da nun bereits $\partial'_{n-2} = \partial_{n-2}$ erhalten worden ist, findet sich allgemein $\partial'_m = \partial_m$, insbesondere also $\partial_0' = \partial_0 = 0$ d. h. d_0' ist durch keine in d_{n-2} aufgehende Primzahl theilbar.

Weil aber jede etwa in d_0' aufgehende Primzahl nothwendig entweder 2 oder eine der in m oder in d_{n-2} enthaltene Primzahl sein müsste, erkennt man aus den erhaltenen Ergebnissen, dass $d_0' = 1$ d. h. dass $b(y_\varrho)$ eine primitive Form sein muss. Nunmehr folgt aus der für jede in d_{n-2} enthaltene Primzahl abgeleiteten Gleichheit

$$\partial'_m = \partial_m, \quad (m = 1, 2, \cdots n-2)$$

dass jede solche Primzahl in o_m' ebenso oft aufgeht wie in o_m; der Gleichung (49) zufolge und weil o_{n-2}' durch $\sigma_1 m$ theilbar ist, bestehen aber die Invarianten $o_1', o_2', \cdots o_{n-3}'$ ebenso wie die Invarianten $o_1, o_2, \cdots o_{n-3}$ nur aus solchen Primzahlen, folglich müssen offenbar

$$o_1' = o_1, \; o_2' = o_2, \cdots o_{n-3}' = o_{n-3}$$

und endlich

$$o_{n-2}' = \sigma_1 o_{n-2} m$$

sein.

Aus alle diesem ergiebt sich endlich, dass die Form $b(y_\varrho)$, wenn sie durch $f(x_\varrho)$ eigentlich darstellbar ist, nur eine primitive Form der Ordnung

$$\text{(I)} \qquad \begin{matrix} o_1, & o_2, & \cdots o_{n-3}, & o_{n-2}\,\varepsilon b \\ \sigma_1, & \sigma_2, & \cdots \sigma_{n-3}, & \sigma_{n-2} \end{matrix}$$

oder, falls n ungerade und $\sigma_1 = 1$ ist, auch eine solche der Ordnung

$$\text{(II)} \qquad \begin{matrix} o_1, & o_2, & \cdots o_{n-3}, & o_{n-2}\,\varepsilon b \\ 2, & 1, & \cdots 1, & 2 \end{matrix}$$

sein kann.

Hiernach lehrt die Beziehung (50), dass die Grössen β_{ix} bis auf das Vorzeichen die Coefficienten der zu $b(y_\varrho)$ reciproken Form mit $n-1$ Veränderlichen sind. Jenachdem nämlich τ oder $\tau - 1$ der Index von $b(y_\varrho)$, jenachdem also b positiv oder negativ ist, wird $\beta(y_\varrho)$ oder $-\beta(y_\varrho)$, d. h. $\varepsilon \cdot \beta(y_\varrho)$ wird die Reciproke von $b(y_\varrho)$ sein.

3) Mit Rücksicht auf die festgestellte Ordnung der Form $b(y_\varrho)$ ist nun leicht einzusehen, dass auch das Geschlecht derselben durch dasjenige der Form $f(x_\varrho)$, durch welche sie darstellbar sein soll, zugleich bestimmt ist. Zur Vereinfachung denken wir wieder $b(y_\varrho)$ als eine (mod. $2b\Delta$) charakteristische Form der Classe, für welche (nr. 16 des sechsten Capitels) $\varepsilon\beta(y_\varrho)$ bei umgekehrter Reihenfolge der Veränderlichen auch eine (mod. $2b\Delta$) charakteristische Form ihrer Classe ist. Heisst $\mathfrak{b}(y_\varrho)$ die so genommene Form $\varepsilon\beta(y_\varrho)$, so nimmt die Congruenz (44) die Gestalt an:

$$\text{(44a)} \quad -\varepsilon o_{n-1} \cdot \mathfrak{b}(y_\varrho) \equiv (\mathfrak{b}_{1n} y_{n-1} + \mathfrak{b}_{2n} y_{n-2} + \cdots + \mathfrak{b}_{n-1,n} y_1)^2 \pmod{b}.$$

Nun ist die Ordnung von $\mathfrak{b}(y_\varrho)$

$$\text{(Ia)} \qquad \begin{matrix} o_{n-2}\,\varepsilon b, & o_{n-3}, & \cdots o_2, & o_1 \\ \sigma_{n-2}, & \sigma_{n-3}, & \cdots \sigma_2, & \sigma_1 \end{matrix}$$

oder

$$\text{(IIa)} \qquad \begin{matrix} o_{n-2}\,\varepsilon b, & o_{n-3}, & \cdots o_2, & o_1 \\ 2, & 1, & \cdots 1, & 2, \end{matrix}$$

jenachdem $b(y_\varrho)$ von der Ordnung (I) oder (II) ist. Da im ersteren Falle die erste σ-Invariante gleich 1, im letzteren Falle aber $\varDelta b$ ungerade ist, wird der Rest von $\mathfrak{b}(y_\varrho)$ (mod. $b\varDelta$) in beiden Fällen die einfache Gestalt haben

$$(51) \qquad \mathfrak{b}(y_\varrho) \equiv \begin{Bmatrix} \mathfrak{b}_{n-1} & 0 & \cdots & 0 \\ 0 & \mathfrak{b}_{n-2} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \mathfrak{b}_1 \end{Bmatrix} \text{(mod. } b\varDelta\text{)},$$

in welcher $\mathfrak{b}_{n-1}$ prim ist gegen $b\varDelta$. In Folge hiervon wird die Congruenz (44a) gleichbedeutend mit dem Systeme der Congruenzen

$$-\varepsilon o_{n-1}\,\mathfrak{b}_i \equiv \mathfrak{b}_{in}^2 \quad (i = 1, 2 \cdots n-1)$$

und

$$0 \equiv \mathfrak{b}_{in}\,\mathfrak{b}_{\varkappa n}\,(i \gtrless \varkappa) \text{ (mod. } b\text{)},$$

die ihrerseits dasselbe besagen wie diese:

$$\left.\begin{matrix} \mathfrak{b}_{1n} \equiv \mathfrak{b}_{2n} \cdots \equiv \mathfrak{b}_{n-2,n} \equiv 0 \\ \mathfrak{b}_1 \equiv \mathfrak{b}_2 \cdots \equiv \mathfrak{b}_{n-2} \equiv 0 \end{matrix}\right\} \text{(mod. } b\text{)}.$$

und

$$(52) \qquad -\varepsilon o_{n-1}\,\mathfrak{b}_{n-1} \equiv \mathfrak{b}_{n-1,n}^2$$

Wir ziehen hieraus sogleich den für die Folge wichtigen Schluss: dass die Anzahl der Wurzeln oder incongruenten Lösungen $\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$ der Congruenz (44) oder (44a) ebenso gross ist, wie die Anzahl der Wurzeln der Congruenz (52) und folglich, falls sie lösbar ist, und wenn β die Anzahl der verschiedenen ungeraden Primzahlen bezeichnet, aus denen die Zahl b besteht, gleich 2^β ist.

Bezeichnen wir weiter, während $m \lesseqgtr n-1$ ist, für die charakteristische Form $b(y_\varrho)$ mit $\sigma'_m\,d'_{m-1}\,b_m$ diejenige Unter-

determinante m^{ten} Grades, die aus den ersten m Zeilen und Spalten ihrer Determinante B gebildet ist, so sind die Zahlen

(53) $$b_1, b_2, \cdots b_{n-2}$$

nicht nur zum Modulus $2b\Delta$ sondern auch jede zu den beiden benachbarten prim; für $m = n - 1$ findet sich

(53a) $$b_{n-1} = (-1)^{\tau}\varepsilon.$$

Wird in gleicher Weise für die Form $g(y_\varrho)$, welche $b(y_\varrho)$ als Bestandtheil enthält, diejenige Unterdeterminante m^{ten} Grades, welche aus den ersten m Zeilen und Spalten der Determinante B gebildet ist, mit $\sigma_m d_{m-1} g_m$ bezeichnet, so findet sich, so lange $m \overline{\overline{<}} n - 2$ ist,

$$\sigma_m g_m = \sigma_m' b_m,$$

während

(54) $$\sigma_{n-1} g_{n-1} = (-1)^{\tau} b$$

ist. Mithin stimmen, wenn $b(y_\varrho)$ zur Ordnung (I) gehört, die Zahlen

$$g_1, g_2, \cdots g_{n-2}$$

mit den Zahlen (53) überein und sind, wie diese, sowohl jede zu den zwei benachbarten, als auch gegen $2b\Delta$ prim; gehört aber $b(y_\varrho)$ zur Ordnung (II), so hat man

$$g_1 = 2b_1, g_2 = b_2, g_3 = 2b_3, \cdots g_{n-2} = 2b_{n-2};$$

da aber jetzt $b\Delta$ ungerade ist, sind diese Zahlen wenigstens wieder prim gegen $b\Delta$. Die Zahlen

(55) $$g_1, g_2, \cdots g_{n-2}, g_{n-1}$$

sind also stets gegen Δ und jede zu den zwei benachbarten prim.

Nun ist zwar die Form $g(y_\varrho)$ nicht nothwendig eine charakteristische Form (mod. 2Δ) der Classe von $f(x_\varrho)$, aber die Zahlen (55) sind gleichzeitig durch sie und ihre primitiven Begleitformen eigentlich darstellbar, und folglich bestimmen die quadratischen Charaktere derselben nach den einzelnen resp. in $o_1, o_2, \cdots o_{n-1}$ aufgehenden ungeraden Primzahlen die Einzelcharaktere, welche der Form $g(y_\varrho)$ oder dem Geschlechte von $f(x_\varrho)$ bezüglich dieser Primzahlen eigen sind, ihre Hauptcharaktere. Andere Charaktere kommen aber,

da Δ als ungerade vorausgesetzt wird, dem Geschlechte von $f(x_\varrho)$ nicht zu, falls $\sigma_1 = 1$ ist.

Ist $\sigma_1 = 2$ also n gerade, ebenso wie b, so treten noch, entsprechend den σ-Invarianten mit geradem Index, Supplementarcharaktere auf. In diesem Falle aber ist die Form $b(y_\varrho)$ von der Ordnung (I), und weil sie als charakteristische Form (mod. $2b\Delta$) gedacht wurde, wird $g(y_\varrho)$ einer Congruenz genügen von folgender Gestalt:

$$g(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0 & \cdots & \cdot & 0 & b_{1n} \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 & \cdots & \cdot & 0 & b_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots 2a', & \mathfrak{A}', & 0 & b_{n-3,n} \\ 0 & 0 & 0 & \cdots \mathfrak{A}', & 2\mathfrak{a}', & 0 & b_{n-2,n} \\ 0 & 0 & 0 & \cdots 0 & 0 & 2\alpha, & b_{n-1,n} \\ b_{1n} & b_{2n} & b_{3n} & \cdots & \cdot & b_{n-1,n}, & b_{nn} \end{Bmatrix} \pmod{4},$$

wo

$$a, \mathfrak{A}, \cdots a', \mathfrak{A}', \alpha$$

ungerade Zahlen sind. Bemerkt man nun, dass die Form

$$2ax_1^2 + 2\mathfrak{A}x_1x_2 + 2\mathfrak{a}x_2^2 + 2b_{1n}x_1x_n + 2b_{2n}x_2x_n + b_{nn}x_n^2$$

durch die unimodulare Substitution

$$x_1 = y_1 + hy_n,\ x_2 = y_2 + ky_n,$$
$$x_n = y_n$$

in die Form

$$2ay_1^2 + 2\mathfrak{A}y_1y_2 + 2\mathfrak{a}y_2^2 + 2b'_{1n}y_1y_n + 2b'_{2n}y_2y_n + b'_{nn}y_n^2$$

übergeht, in welcher

$$b'_{1n} = 2ah + \mathfrak{A}k + b_{1n}$$
$$b'_{2n} = \mathfrak{A}h + 2\mathfrak{a}k + b_{2n}$$

ist, so lassen sich, da die Determinante

$$2a \cdot 2\mathfrak{a} - \mathfrak{A}^2$$

ungerade ist, die ganzen Zahlen h, k so wählen, dass

$$b'_{1n} \equiv 0,\ b'_{2n} \equiv 0 \pmod{4}$$

wird; und indem man dies Verfahren zu wiederholten Malen zur Anwendung bringt, führt man $g(y_\varrho)$ in eine äquivalente Form $g'(y_\varrho)$ über, welche der Congruenz

$$g'(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0 \cdots & \cdot & 0 & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 \cdots & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 \cdots 2a', & \mathfrak{A}', & 0 & 0 \\ 0 & 0 & 0 \cdots \mathfrak{A}', & 2\mathfrak{a}', & 0 & 0 \\ 0 & 0 & 0 \cdots 0 & 0 & 2\alpha & \beta \\ 0 & 0 & 0 \cdots 0 & 0 & \beta & \gamma \end{Bmatrix} \pmod{4}$$

Genüge leistet und wo nun γ wegen $\sigma_1 = 2$ gerade und β wegen der ungeraden Determinante Δ ungerade sein muss. Man sieht, dass diese Form ein Hauptrepräsentant für die Classe von $f(x_\varrho)$ ist. Demnach sind*) die supplementären Charaktere des Geschlechts von $f(x_\varrho)$ die Werthe der Symbole

$$(56)\quad \begin{cases} (-1)^{\frac{g_2'-1}{2}} = (-1)^{\frac{g_2-1}{2}}, \; (-1)^{\frac{g_4'-1}{2}} = (-1)^{\frac{g_4-1}{2}}, \\ \qquad \cdots (-1)^{\frac{g_{n-2}'-1}{2}} = (-1)^{\frac{g_{n-2}-1}{2}}. \end{cases}$$

Andererseits kommen der Form $b(y_\varrho)$ zunächst als **Hauptcharaktere** diejenigen quadratischen Charaktere zu, welche die Zahlen (53) mit Bezug auf die resp. in $o_1, o_2, \cdots o_{n-2}$ aufgehenden ungeraden Primzahlen besitzen, sowie ausserdem noch die quadratischen Charaktere der Zahl b_{n-2} mit Bezug auf die Primfaktoren von b. Gehört nun **erstens** $b(y_\varrho)$ zur Ordnung (I) und ist $\sigma_1 = 1$, so hat $b(y_\varrho)$ keine weiteren Einzelcharaktere; jene aber, welche sich auf die Primfaktoren von $o_1, o_2, \cdots o_{n-2}$ beziehen, sind, da die Zahlen $g_1, g_2, \cdots g_{n-2}$ in diesem Falle mit den Zahlen (53) übereinstimmen, gleich den entsprechenden Charakteren des Geschlechts von $f(x_\varrho)$; und diejenigen der Zahl

$$(57)\qquad b_{n-2} = \beta_{n-1,n-1}$$

mit Bezug auf die Primfaktoren von b sind wegen der aus (44) entspringenden Congruenz

$$(58)\qquad -o_{n-1} \cdot (-1)^r \beta_{n-1,n-1} \equiv \mathfrak{b}_{n-1,n}^2 \pmod{b}$$

gleichwerthig mit den quadratischen Charakteren der Zahl $(-1)^{r+1} \cdot o_{n-1}$ bezüglich derselben Primfaktoren, also durch

*) S. die Anmerkung S. 467 zu nr. 13 des sechsten Capitels.

die Ordnung der Form $f(x_\varrho)$ vollkommen bestimmt. — Ist $\sigma_1 = 2$, so gilt für die Hauptcharaktere von $b(y_\varrho)$ das eben Gesagte, aber, weil in diesem Falle für $b(y_\varrho)$ eine Congruenz von der Gestalt:

$$b(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0 \cdots & & \cdot & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 \cdots & & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 \cdots & 2a', & \mathfrak{A}', & 0 \\ 0 & 0 & 0 \cdots & \mathfrak{A}', & 2\mathfrak{a}', & 0 \\ 0 & 0 & 0 \cdots & 0 & 0 & 2\alpha \end{Bmatrix} \pmod{4}$$

besteht, treten zu ihnen noch die **Supplementarcharaktere**

$$(59) \qquad (-1)^{\frac{b_2-1}{2}}, (-1)^{\frac{b_4-1}{2}}, \cdots (-1)^{\frac{b_{n-4}-1}{2}}$$

hinzu; diese sind jedoch den entsprechenden Charakteren (56) gleich also ebenfalls durch das Geschlecht von $f(x_\varrho)$ mitbestimmt.

Gehört aber **zweitens** $b(y_\varrho)$ zur Ordnung (II), so gilt noch immer bezüglich der Hauptcharaktere von $b(y_\varrho)$ im wesentlichen dasselbe wie vorher, nur dass an Stelle der Gleichung (57) die andere:

$$(57') \qquad 2b_{n-2} = \beta_{n-1, n-1}$$

zu setzen ist und dass die Charaktere der Zahlen (53) mit Bezug auf die Primfaktoren von $o_1, o_2, \cdots o_{n-2}$ nicht mehr denjenigen der Zahlen (55) gleich, aber doch durch letztere wesentlich bestimmt sind. Den Supplementarcharakteren

$$(59') \qquad (-1)^{\frac{b_2-1}{2}}, (-1)^{\frac{b_4-1}{2}}, \cdots (-1)^{\frac{b_{n-3}-1}{2}}$$

entsprechen zwar jetzt keine Charaktere der Form $f(x_\varrho)$; da jedoch in diesem Falle

$$b(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0 \cdots 0 & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0 \cdots 0 & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 \cdots 2a', & \mathfrak{A}' \\ 0 & 0 & 0 \cdots \mathfrak{A}', & 2\mathfrak{a}' \end{Bmatrix} \pmod{4}$$

gesetzt werden kann, sind die bezeichneten Charaktere ver-

mittelst der Congruenzen

$$d_{2m-1} \cdot b_{2m} \equiv (-1)^m \pmod{4}$$

durch die Form $f(x_\varrho)$ ebenfalls völlig bestimmt.

Und somit gelangt man, die sämmtlichen, bezüglich der Form $b(y_\varrho)$ angestellten Betrachtungen zusammenfassend, zu folgendem Endergebnisse:

Damit eine Form $b(y_\varrho)$ mit $n-1$ Veränderlichen durch die primitive Form $f(x_\varrho)$ mit n Veränderlichen und von der Ordnung

$$\tau, \begin{matrix} o_1, o_2, \cdots o_{n-2}, o_{n-1} \\ \sigma_1, \sigma_2, \cdots \sigma_{n-2}, \sigma_{n-1} \end{matrix}$$

eigentlich darstellbar sei, muss sie eine Determinante haben von der Form

$$(-1)^\tau \cdot d_{n-2} b,$$

wo die quadratischen Charaktere von b der Bedingungsgleichung (38) unterworfen sind, wenn $b = \varepsilon \sigma_1 m$ gesetzt wird *und m prim gegen 2Δ ist*, und muss in derselben Voraussetzung eine primitive Form sein, deren Reciproke, mit $-\varepsilon o_{n-1}$ multiplicirt, quadratischer Rest von b ist, und sie kann zudem nur *einem* — im Falle eines ungeraden n und wenn $\sigma_1 = 1$ ist, nur *zwei* — durch das Geschlecht von $f(x_\varrho)$ völlig bestimmten Geschlechtern von Formen angehörig sein, die als die Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$, entsprechend den Ordnungen (I) und (II), bezeichnet werden mögen.

8. Umgekehrt seien

$$o_1, o_2, \cdots o_{n-2}, o_{n-1}$$

gegebene ungerade Zahlen,

$$d_h = o_1^h o_2^{h-1} \cdots o_{h-1}^2 o_h$$
$$(h = 1, 2, \cdots n-1)$$

und $\Delta = (-1)^\tau \cdot d_{n-1}$; ferner sei $b = \varepsilon \sigma m$, wo $\varepsilon = \pm 1$, $\sigma = 1$ oder 2 und $m > 0$ prim zu 2Δ, endlich $\tau' = \tau$ oder $\tau - 1$, jenachdem b positiv oder negativ ist. Man betrachte die Ordnung O':

$$\tau', \begin{matrix} o_1, o_2, \cdots o_{n-3}, o_{n-2}\varepsilon b \\ \sigma_1, \sigma_2, \cdots \sigma_{n-3}, \sigma_{n-2} \end{matrix}$$

von Formen mit $n-1$ Veränderlichen. Damit sie wirklich vorhanden sei, müssen die σ-Invarianten durch nr. 6 des sechsten Capitels bestimmte Werthe haben, insbesondere, wenn $\sigma = 1$ und n ungerade ist, entweder

$$\sigma_1 = \sigma_2 = \cdots = \sigma_{n-2} = 1$$

oder

$$\sigma_1 = 2,\ \sigma_2 = 1,\ \sigma_3 = 2 \cdots \sigma_{n-2} = 2$$

sein.

Gesetzt, sie existire dann wirklich und $b(y_\varrho)$ sei eine (primitive) Form dieser Ordnung, also ihre Determinante

$$(-1)^{\tau'} d_{n-2} \cdot \varepsilon b = (-1)^{\tau} d_{n-2} b,$$

so lässt sich zunächst aus den voraufgehenden Betrachtungen schliessen, dass nur ein ganz bestimmtes Geschlecht von Formen mit n Veränderlichen und den letzten beiden d-Invarianten d_{n-2}, d_{n-1} vorhanden sein kann, durch deren Formen eine eigentliche Darstellung von $b(y_\varrho)$ denkbar ist. Denn, sei $f(x_\varrho)$ eine solche Form, deren Ordnung

$$\theta \begin{matrix} o_1', & o_2', & \cdots o_{n-3}', & o_{n-2}', & o_{n-1}' \\ \sigma_1', & \sigma_2', & \cdots \sigma_{n-3}', & \sigma_{n-2}', & \sigma_{n-1}' \end{matrix}$$

heisse, so muss zunächst $\theta = \tau$ und die Ordnung O' mit Bezug auf $f(x_\varrho)$ entweder eine Ordnung (I) oder eine Ordnung (II) sein. Man schliesst in beiden Fällen

$$o_1' = o_1,\ o_2' = o_2,\ \cdots o_{n-2}' = o_{n-2}$$

also wegen

$$d_{n-1} = o_1^{n-1} o_2^{n-2} \cdots o_{n-2}^2 o_{n-1} = o_1'^{\,n-1} o_2'^{\,n-2} \cdots o_{n-2}'^{\,2} o_{n-1}'$$

auch

$$o_{n-1}' = o_{n-1};$$

ferner im ersten Falle

$$\sigma_1' = \sigma_1,\ \sigma_2' = \sigma_2,\ \cdots \sigma_{n-2}' = \sigma_{n-2},$$

womit zugleich auch σ_{n-1}' völlig bestimmt ist, weil die σ-Invarianten der Form $f(x_\varrho)$ der ungeraden Determinante wegen entweder nur sämmtlich gleich 1, oder abwechselnd gleich 2 und 1 sein können; das Erstere wird eintreten, wenn n und b ungerade sind. Im zweiten Falle, der sich nur ereignen kann, wenn n und b ungerade sind, müsste $\sigma_1' = \sigma = 1$ sein

und somit würden sämmtliche σ-Invarianten der Form $f(x_\varrho)$ gleich 1. Da somit der zweite Fall, sobald er möglich ist, zu derselben Ordnung führt, wie der erste, steht zunächst die Ordnung der Form $f(x_\varrho)$ vollkommen fest.

Dann aber ergeben sich auch nach der obigen Auseinandersetzung aus den Charakteren der Form $b(y_\varrho)$ sämmtliche Charaktere der Form $f(x_\varrho)$ unmittelbar, mit Ausnahme derjenigen Hauptcharaktere, welche auf die Primfaktoren von o_{n-1} bezüglich sind, sowie des im Falle $\sigma_1' = 2$ auftretenden supplementären Charakters

$$(-1)^{\frac{o'_{n-2}-1}{2}}.$$

Indessen bestimmen sich die supplementären Charaktere (56) nach nr. 14 des sechsten Capitels durch einander und so wird auch dieser durch die übrigen unzweideutig definirt sein; bezüglich der Primfaktoren p_{n-1} von o_{n-1} aber besteht die Bedingungsgleichung

$$\left(\frac{b}{p_{n-1}}\right) = \left(\frac{\mathfrak{f}_1'}{p_{n-1}}\right) = \left(\frac{(-1)^\tau f'_{n-1}}{p_{n-1}}\right),$$

sodass auch diese Einzelcharaktere der Form $f(x_\varrho)$ durch die Form $b(y_\varrho)$ völlig bestimmt sind.

Wird nun vorausgesetzt, dass für jede in b aufgehende Primzahl q die Bedingung

$$\left(\frac{b_{n-2}}{q}\right) = \left(\frac{(-1)^{\tau+1} o_{n-1}}{q}\right)$$

erfüllt, dass also

$$(-1)^{\tau+1} o_{n-1} b_{n-2} \text{ quadratischer Rest von } b$$

sei, so ist das bezeichnete Geschlecht von Formen mit n Veränderlichen auch wirklich d. h. eine Form eines solchen Geschlechts thatsächlich vorhanden. Beim Nachweis dieser Behauptung darf man wieder $b(y_\varrho)$ als eine (mod. $2b\varDelta$) charakteristische Form ihrer Classe voraussetzen. Alsdann besteht für die mit $\mathfrak{b}(y_\varrho)$ bezeichnete Form die Congruenz (51), aus welcher

$$\mathfrak{b}_{n-1} \equiv \varepsilon \cdot (-1)^\tau \beta_{n-1,n-1} \equiv \varepsilon \cdot (-1)^\tau b_{n-2} \pmod{b}$$

hervorgeht. Der gemachten Voraussetzung zufolge wird also

$$- \varepsilon\, o_{n-1} \mathfrak{b}_{n-1} \text{ quadratischer Rest von } b$$

mithin die Congruenz (52) und in Folge davon auch die Congruenz (44a) oder diese andere:

$$(60) \qquad - o_{n-1} \cdot \beta(y_\varrho) \equiv (\mathfrak{b}_{1n} y_1 + \mathfrak{b}_{2n} y_2 + \cdots + \mathfrak{b}_{n-1,n} y_{n-1})^2 \pmod{b}$$

auflösbar sein. Seien nun die Zahlen

$$\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$$

irgend eine bestimmte Wurzel dieser Congruenz, so giebt es ihr zufolge für jede Combination $i, \varkappa$ aus der Reihe

$$1, 2, 3, \cdots n-1$$

eine ganze Zahl $\mathfrak{b}_{i\varkappa}$, welche der Gleichung

$$(61) \qquad (-1)^\tau o_{n-1} \cdot \beta_{i\varkappa} = b \cdot \mathfrak{b}_{i\varkappa} - \mathfrak{b}_{in} \mathfrak{b}_{\varkappa n}$$

genügt, und für jede solche Combination wird

$$\mathfrak{b}_{\varkappa i} = \mathfrak{b}_{i\varkappa}$$

sein; ausserdem werde $\mathfrak{b}_{ni} = \mathfrak{b}_{in}$, $\mathfrak{b}_{n\varkappa} = \mathfrak{b}_{\varkappa n}$ gesetzt und

$$(62) \qquad \mathfrak{b}_{nn} = b.$$

Man bestimme nun die Zahlen

$$b_{n1} = b_{1n}, b_{n2} = b_{2n}, \cdots b_{n,n-1} = b_{n-1,n}$$

durch die $n-1$ Gleichungen:

$$(63) \quad \beta_{1\varkappa} b_{n1} + \beta_{2\varkappa} b_{n2} + \cdots + \beta_{n-1,\varkappa} b_{n,n-1} = (-1)^\tau \cdot \frac{d_{n-2}}{d_{n-3}} \cdot \mathfrak{b}_{\varkappa n} \quad (\varkappa = 1, 2, \cdots n-1)$$

und die Zahl b_{nn} durch folgende Gleichung

$$(64) \qquad \mathfrak{b}_{1n} b_{1n} + \mathfrak{b}_{2n} b_{2n} + \cdots + \mathfrak{b}_{nn} b_{nn} = \frac{d_{n-1}}{d_{n-2}},$$

wo $d_{n-1}, d_{n-2}, d_{n-3}$ durch die Grössen $o_1, o_2, \cdots o_{n-1}$ in gleicher Weise wie früher bestimmt gedacht werden. Wir wollen den Nachweis führen, dass die so definirten Zahlen bestimmte ganze Zahlen sind. Indem wir die n-gliedrige Determinante

$$(65) \qquad | b_{i\varkappa} | = B$$

setzen, erhalten wir die Beziehung

$$\frac{\partial^2 B}{\partial b_{nn} \partial b_{i\varkappa}} = \frac{\partial \mathrm{B}}{\partial b_{i\varkappa}} = d_{n-3} \cdot \beta_{i\varkappa},$$

folglich ist die Determinante der Gleichungen (63) bis auf eine Potenz von d_{n-3}, welche als Faktor hinzutritt, die Adjungirte der Determinante B also von Null verschieden und folglich liefern jene Gleichungen für die Grössen

$$b_{n1},\ b_{n2},\ \cdots b_{n-1,n}$$

jedenfalls bestimmte endliche Werthe. Man kann die Gleichungen aber auch folgendermassen schreiben:

$$(63\text{a})\qquad (-1)^r\cdot\frac{\partial B}{\partial b_{\varkappa n}} = d_{n-2}\cdot \mathfrak{b}_{\varkappa n}$$
$$(\varkappa = 1, 2, \cdots n-1)$$

und aus

$$\frac{\partial B}{\partial b_{nn}} = \mathsf{B} = (-1)^r d_{n-2}\cdot b$$

findet sich wegen (62)

$$(63\text{b})\qquad (-1)^r\cdot\frac{\partial B}{\partial b_{nn}} = d_{n-2}\cdot \mathfrak{b}_{nn}.$$

Vermittelst dieser Formeln erhält man aus (64) für die Determinante B den Werth

$$B = \varDelta = (-1)^r d_{n-1}.$$

Vergleicht man folglich die Gleichung (61) mit der Determinantenformel

$$B\cdot\frac{\partial^2 B}{\partial b_{nn}\partial b_{i\varkappa}} = \frac{\partial B}{\partial b_{i\varkappa}}\,\frac{\partial B}{\partial b_{nn}} - \frac{\partial B}{\partial b_{in}}\,\frac{\partial B}{\partial b_{n\varkappa}},$$

so erschliesst man für jede Combination $i, \varkappa$ der Reihe

$$1, 2, \cdots n-1$$

noch folgende Formel:

$$(63\text{c})\qquad (-1)^r\cdot\frac{\partial B}{\partial b_{i\varkappa}} = d_{n-2}\cdot \mathfrak{b}_{i\varkappa}.$$

In Folge der Gleichungen (63 a, b, c) finden also die nachstehenden statt, in welchen i je eine Zahl, i, h jede Combination zweier Zahlen der Reihe $1, 2, 3, \cdots n$ bedeuten:

$$(64\text{a})\qquad \begin{cases} b_{i1}\mathfrak{b}_{h1} + b_{i2}\mathfrak{b}_{h2} + \cdots + b_{in}\mathfrak{b}_{hn} = 0 \\ b_{i1}\mathfrak{b}_{i1} + b_{i2}\mathfrak{b}_{i2} + \cdots + b_{in}\mathfrak{b}_{in} = \dfrac{d_{n-1}}{d_{n-2}}. \end{cases}$$

Denkt man nun i zunächst als eine der Zahlen $1, 2, \cdots n-1$, so zeigen diese Gleichungen, dass

$$b_{in}\mathfrak{b}_{1n},\ b_{in}\mathfrak{b}_{2n},\ \cdots b_{in}\mathfrak{b}_{nn} = b_{in}\cdot b$$

ganze Zahlen sind; weil aber die Zahlen $\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$ wegen der Congruenz (44) mit b keinen gemeinsamen Theiler haben (denn $\varepsilon\beta(y_\varrho)$ ist als Reciproke von $b(y_\varrho)$ eine primitive Form), muss auch die Zahl b_{in} d. h. jede der Zahlen b_{1n}, $b_{2n}, \cdots b_{n-1,n}$ eine ganze Zahl sein. Nimmt man daher jetzt in den Gleichungen (64a) $i = n$ an, so beweist man aus ihnen auf gleiche Weise dasselbe auch noch für die Zahl b_{nn}.

Durch diese Betrachtung ist aus der Form $b(y_\varrho)$ eine andere primitive Form

$$g(y_\varrho) = \sum_{(\alpha,\beta = 1, 2, \cdots n)} b_{\alpha\beta}\, y_\alpha\, y_\beta \tag{65}$$

mit ganzzahligen Coefficienten hergeleitet worden, deren letzte d-Invariante d_{n-1} ist. Die Formeln (63a, b, c) zeigen zudem, da die Zahlen

$$\mathfrak{b}_{1n},\ \mathfrak{b}_{2n},\ \cdots \mathfrak{b}_{n-1,n},\ \mathfrak{b}_{nn} = b$$

ohne gemeinsamen Theiler sind, dass d_{n-2} die vorletzte d-Invariante von $g(y_\varrho)$ ist. Somit ist

$$\mathfrak{g}(y_\varrho) = \sum_{(\alpha,\beta = 1, 2, \cdots n)} \mathfrak{b}_{\alpha\beta}\, y_\alpha\, y_\beta \tag{66}$$

ihre Reciproke. Da die erstere dieser Formen die Form $b(y_\varrho)$ als Bestandtheil enthält, ist $b(y_\varrho)$ eigentlich durch sie darstellbar und deshalb ist $g(y_\varrho)$ eine Form des anfangs bezeichneten ganz bestimmten Geschlechts, dessen wirkliche Existenz dadurch bewiesen ist.

9. Nachdem wir diesen Punkt festgestellt haben, wenden wir uns nun zu der Frage, inwieweit die in nr. 7 angegebenen Bedingungen, welche die Form $b(y_\varrho)$ erfüllen muss, um durch $f(x_\varrho)$ eigentlich darstellbar zu sein, hierzu auch ausreichend sind.

Nehmen wir also an, $b(y_\varrho)$ sei eine primitive Form mit $n-1$ Veränderlichen, welche jenen Bedingungen genügt also dem durch $f(x_\varrho)$ völlig bestimmten Geschlechte $\Gamma_{(\mathrm{I})}$ — oder auch, falls es zulässig ist, dem Geschlechte $\Gamma_{(\mathrm{II})}$ — angehört. Den Voraussetzungen gemäss ist die Congruenz (44) auflösbar und hat 2^β Wurzeln, wenn b durch β verschiedene ungerade

Primzahlen theilbar ist. Man gelangt mithin genau wie vorher, wenn $\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$ irgend eine dieser Wurzeln bedeuten, zu einer Form $g(y_\varrho)$, von welcher $b(y_\varrho)$ ein Bestandtheil ist, und in deren Reciproken $\mathfrak{g}(y_\varrho)$ die Zahlen

$$\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}, \mathfrak{b}_{nn} = b$$

die letzte Zeile (Spalte) des Coefficientensystems ausmachen. Das Geschlecht von $g(y_\varrho)$ kann kein anderes sein, als das der gegebenen Form $f(x_\varrho)$. Man erhält so, den verschiedenen Wurzeln der Congruenz (44) entsprechend 2^δ Formen $g(y_\varrho)$ des Geschlechts G von $f(x_\varrho)$. Da nun nach nr. 6 jede eigentliche Darstellung von $b(y_\varrho)$ durch die Form $f(x_\varrho)$ zu einer bestimmten der 2^δ Wurzeln gehört, und, wenn

$$\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$$

diese Wurzel ist, die entsprechende Form $g(y_\varrho)$ mit $f(x_\varrho)$ äquivalent sein muss und die zu der Wurzel gehörigen Darstellungen aus den Transformationen von $f(x_\varrho)$ in $g(y_\varrho)$ gefunden werden, ergiebt sich folgende Regel, um alle etwa vorhandenen eigentlichen Darstellungen von $b(y_\varrho)$ durch $f(x_\varrho)$ zu ermitteln:

Man stelle für jede Wurzel der Congruenz (44) die in der vorher angegebenen Weise bestimmte Form $g(y_\varrho)$ von n Veränderlichen auf. Es giebt dann keine eigentlichen Darstellungen von $b(y_\varrho)$ durch $f(x_\varrho)$, wenn $f(x_\varrho)$ keiner dieser Formen äquivalent ist. Ist dagegen $f(x_\varrho)$ einer von ihnen, derjenigen etwa, welche der Wurzel

$$\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$$

entspricht, äquivalent, so giebt es Darstellungen von $b(y_\varrho)$ durch $f(x_\varrho)$, welche zu dieser Wurzel gehören, und sie werden sämmtlich, jede einmal, gefunden, wenn man alle Transformationen von $f(x_\varrho)$ in jene Form $g(y_\varrho)$ aufsucht und die letzte Veränderliche in ihnen gleich Null setzt. Wird dies bezüglich aller der 2^δ Formen ausgeführt, denen etwa $f(x_\varrho)$ äquivalent ist, so erhält man die sämmtlichen überhaupt möglichen eigentlichen Darstellungen der Form $b(y_\varrho)$ durch die gegebene Form $f(x_\varrho)$ und jede von ihnen (vgl. (47)) einmal.

Man erkennt hieraus, dass die vollständige Lösung der

Aufgabe, alle möglichen eigentlichen Darstellungen der Form $b(y_\varrho)$ mit $n-1$ Variabeln durch eine Form $f(x_\varrho)$ mit n Variabeln zu finden, die Lösung zweier anderen voraussetzt: 1) zu entscheiden, ob $f(x_\varrho)$ einer Form $g(y_\varrho)$ äquivalent ist oder nicht, und 2) im ersteren Falle alle ganzzahligen Transformationen jener Form in diese letztere zu ermitteln. Soweit diese beiden Aufgaben überhaupt seither ihre Erledigung gefunden haben, werden sie im dritten Theile dieses Werkes gelöst werden, auf welchen somit hier zu verweisen ist.

In demselben Theile wird auch der Nachweis geliefert werden, dass die Anzahl der Classen aller Formen eines gegebenen Geschlechts endlich ist. Demnach ist es möglich, sämmtliche Classen durch eine endliche Anzahl von Formen zu repräsentiren, indem man dazu aus jeder Classe eine Form nach Belieben herausgreift. Ein System solcher repräsentirender Formen heisst ein Formensystem des Geschlechts. — Handelt es sich nun darum, alle etwa vorhandenen eigentlichen Darstellungen einer Form $b(y_\varrho)$ nicht sowohl durch eine bestimmte Form $f(x_\varrho)$, sondern durch alle Formen eines Formensystems eines gegebenen Geschlechts G zu ermitteln, so wird zunächst festzustellen sein, ob die Form $b(y_\varrho)$ die zu solcher Darstellung erforderlichen Bedingungen (S. 581) erfüllt. Ist dies der Fall, so hat man offenbar nur ein Formensystem

$$f_1(x_\varrho),\ f_2(x_\varrho),\ f_3(x_\varrho),\ \cdots \tag{67}$$

des Geschlechts G aufzustellen und nun für jede Form dieses Systems das Verfahren durchzuführen, das wir soeben bezüglich der Form $f(x_\varrho)$ auseinandergesetzt haben.

10. Hiermit verbinden wir die in nr. 4 gegebene Regel zur Ermittelung aller eigentlichen Darstellungen einer Zahl durch eine Form $f(x_\varrho)$ und lösen die Aufgabe: sämmtliche verschiedenen eigentlichen Darstellungen einer Zahl b durch die Repräsentanten eines gegebenen Geschlechts von Formen mit n Veränderlichen zu finden. Wir denken uns vor allem das Formensystem dieses Geschlechts aufgestellt. Da jedem gegebenen Geschlechte ein anderes ent-

spricht, dessen Formen zu denen des ersteren reciprok sind, darf man die Repräsentanten des gegebenen Geschlechts $\mathfrak{G}$:

$$\text{(68)} \qquad \mathfrak{f}_1(x_\varrho),\ \mathfrak{f}_2(x_\varrho),\ \mathfrak{f}_3(x_\varrho),\ \cdots$$

als die Reciproken der Repräsentanten

$$\text{(69)} \qquad f_1(x_\varrho),\ f_2(x_\varrho),\ f_3(x_\varrho),\ \cdots$$

eines bestimmten anderen Geschlechts G auffassen, wenn man bedenkt, dass zwei äquivalenten Formen auch zwei äquivalente reciproke Formen entsprechen und umgekehrt. Soll nun unsere Aufgabe überhaupt lösbar, nämlich b durch irgend eine Form der Reihe (68) eigentlich darstellbar sein, so ist durchaus erforderlich, dass b durch σ_{n-1} d. h. unter der Voraussetzung einer ungeraden Determinante Δ durch σ_1 theilbar:

$$b = \varepsilon\sigma_1 m$$

sei; wir nehmen diese Bedingung für erfüllt an und beschränken uns dann auf den Fall, wo m prim ist gegen 2Δ. Ferner müssen der Zahl b diejenigen quadratischen Charaktere zukommen, welche durch das Geschlecht $\mathfrak{G}$ bedingt sind, sodass für jede in o_{n-1} (der ersten o-Invariante dieses Geschlechts) aufgehende Primzahl p_{n-1} die Bedingungsgleichung (38)

$$\left(\frac{b}{p_{n-1}}\right) = \left(\frac{\mathfrak{f}_1'}{p_{n-1}}\right)$$

erfüllt sein muss. Nach der in nr. 4 gegebenen Regel werden dann sämmtliche eigentliche Darstellungen dieser Zahl b durch die Formen (68) gefunden, wenn man die adjungirten eigentlichen Darstellungen aller Formen mit $n-1$ Veränderlichen und der Determinante $(-1)^\varepsilon d_{n-2} \cdot b$ durch die Formen (69) ermittelt. Da aber nach den letzten Untersuchungen nur diejenigen Formen mit $n-1$ Veränderlichen, welche einem resp. zwei durch das Geschlecht $\mathfrak{G}$ oder G vollkommen bestimmten Geschlechte $\Gamma_{(\mathrm{I})}$ resp. $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$ angehören, einer Darstellung durch die Formen (69) fähig, andererseits nach eben jener Regel nur die Darstellungen nicht äquivalenter Formen zu berücksichtigen sind, braucht man nur die vorhandenen Repräsentanten des Geschlechts $\Gamma_{(\mathrm{I})}$ resp. der zwei Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$ in Betracht zu ziehen. Ist dann $b(y_\varrho)$ irgend einer dieser Repräsentanten und $\varepsilon\beta(y_\varrho)$ die

zugehörige Reciproke, so gehört jede eigentliche Darstellung von $b(y_\varrho)$ durch die Formen des Geschlechts G zu einer Wurzel der Congruenz (44). Den 2^β Wurzeln

$$\mathfrak{b}_{1n}, \mathfrak{b}_{2n}, \cdots \mathfrak{b}_{n-1,n}$$

derselben entsprechend giebt es 2^β Formen

$$g_1(y_\varrho), g_2(y_\varrho), \cdots g_{2^\beta}(y_\varrho) \tag{70}$$

des Geschlechts G, welche $b(y_\varrho)$ als Bestandtheil enthalten. Jede von ihnen, $g_i(y_\varrho)$, muss einem der Repräsentanten (69), etwa $f_\varkappa(x_\varrho)$ äquivalent sein, demjenigen nämlich, durch welchen — und durch welchen allein — $b(y_\varrho)$ eigentliche Darstellungen gestattet, die zu der $g_i(y_\varrho)$ entsprechenden Congruenzwurzel gehören; und man erhält sämmtliche eigentliche Darstellungen

$$x_\varrho = q_{\varrho 1}y_1 + q_{\varrho 2}y_2 + \cdots + q_{\varrho, n-1}y_{n-1} \qquad (\varrho = 1, 2, \cdots n) \tag{71}$$

von $b(y_\varrho)$ durch diesen Repräsentanten, welche zu der der Form $g_i(y_\varrho)$ entsprechenden Wurzel gehören, wenn man sämmtliche Transformationen

$$x_\varrho = q_{\varrho 1}y_1 + q_{\varrho 2}y_2 + \cdots + q_{\varrho, n-1}y_{n-1} + q_{\varrho n}y_n \qquad (\varrho = 1, 2, 3, \cdots n)$$

von $f_\varkappa(x_\varrho)$ in $g_i(y_\varrho)$ aufstellt und die letzte Veränderliche y_n in ihnen gleich Null setzt; die Menge derselben ist also gerade so gross, wie die Menge der Transformationen der Form $f_\varkappa(x_\varrho)$ in sich selbst. Diese eigentlichen Darstellungen (71) von $b(y_\varrho)$ durch $f_\varkappa(x_\varrho)$ zerfallen aber in Complexe äquivalenter Darstellungen, deren jeder so viel Darstellungen enthält, als $b(y_\varrho)$ Transformationen in sich selber gestattet, und man erhält alle der gedachten Wurzel der Congruenz (44) entsprechenden eigentlichen Darstellungen von b durch die Form $f_\varkappa(x_\varrho)$, wenn man aus jedem solchen Complexe äquivalenter Darstellungen von $b(y_\varrho)$ durch $f_\varkappa(x_\varrho)$ nur eine Darstellung (71) wählt und dann

$$x_1 = Q_{1n}, x_2 = Q_{2n}, \cdots x_n = Q_{nn} \tag{72}$$

setzt. Wird dies für jede Form $b(y_\varrho)$ des Geschlechts $\Gamma_{(I)}$ resp., wenn das Geschlecht $\Gamma_{(II)}$ zulässig ist, auch dieses letzteren Geschlechts und für jede der ihr entsprechenden Formen (70) in gleicher Weise zur Ausführung gebracht, so muss man nach

nr. 4 und 6 sämmtliche eigentliche Darstellungen der Zahl b durch die Repräsentanten (68) des Geschlechts $\mathfrak{G}$, jede einmal, erhalten.

11. An die Darstellungstheorie knüpft sich die Frage, ob die als denkbar bezeichneten Geschlechter von Formen mit n Veränderlichen auch wirklich vorhanden sind d. h. thatsächlich Formen enthalten. Jedes denkbare Geschlecht der Ordnung O:

$$\tau,\ \begin{matrix} o_1, o_2, \cdots o_{n-2}, o_{n-1} \\ \sigma_1, \sigma_2, \cdots \sigma_{n-2}, \sigma_{n-1} \end{matrix}$$

wird durch die Werthe gewisser Einheiten definirt, welche gemäss der Möglichkeitsbedingung d. i., wenn man

$$(73) \qquad (-1)^{\left[\frac{\tau}{2}\right]+\psi(o,n-1)} \cdot \prod_{m=1}^{n-1}\left(\frac{f'_m}{e_m}\right) = \Pi$$

setzt, gemäss der Gleichung

$$(74) \qquad \Pi = 1$$

von einander abhängig sind. Es fragt sich mithin, ob, wenn man diese Einheiten in beliebiger Weise so wählt, dass letztere Bedingung erfüllt ist, es wirklich ein Geschlecht von Formen mit n Veränderlichen giebt, deren Einzelcharaktere jenen Einheiten gleich sind. Wir verfolgen diese Frage hier ausschliesslich für den Fall, wo die Determinante der Formen ungerade und die erste σ-Invariante gleich 1 ist, da für andere Fälle eine breitere Grundlage erforderlich wäre, als sie im Vorigen entwickelt worden ist; in dem gedachten Falle ist sie zu bejahen. Die Zahlen e_m sind dann mit den Invarianten o_m identisch, also

$$(75) \begin{cases} \psi(o, n-1) \\ = \sum_{m=1}^{n-1} \frac{1}{4}(f'_m - 1)(o_m + 1) + \sum_{m=1}^{n-1} \frac{1}{4}(f'_m - 1)(f'_{m+1} - 1). \end{cases}$$

Gesetzt, $f(x_\varrho)$ wäre eine Form des fraglichen Geschlechts und $f'(y_\varrho)$ eine (mod. 2Δ) charakteristische Form ihrer Classe, so würde man vermittelst der letzteren die Ausdrücke, welche als Einzelcharaktere bezeichnet wor-

den sind, bilden können. Da $\sigma_1 = 1$ vorausgesetzt ist, sind diese Ausdrücke nur die folgenden Hauptcharaktere:

$$\left(\frac{f'_m}{p_m}\right) \qquad (C)$$
$$(m = 1, 2, \cdots n-1)$$

bezüglich aller in o_m aufgehenden Primfaktoren p_m. Setzte man die letzte Veränderliche in $f'(y_\varrho)$ gleich Null, so entstände eine Form $b(y_\varrho)$ mit $n-1$ Veränderlichen, deren erster Coefficient ungerade, deren erste σ-Invariante also gleich 1 wäre, und diese Form wäre durch $f'(y_\varrho)$ also auch durch $f(x_\varrho)$ eigentlich darstellbar. Nennt man ihre Determinante

$$(-1)^\tau d_{n-2} b,$$

so ergiebt sich

$$(-1)^\tau d_{n-2} b = \sigma_{n-1} d_{n-2} f'_{n-1},$$

woraus, da $\sigma_{n-1} = 1$ ist, hervorgeht, dass

$$b = (-1)^\tau f'_{n-1}$$

also zu 2Δ prim ist. Daher entspräche dem hypothetischen Geschlechte G der Form $f(x_\varrho)$ (nach den Auseinandersetzungen in nr. 7) ein anderes zugleich mit ihm vorhandenes bestimmtes Geschlecht $\Gamma_{(1)}$ von Formen mit $n-1$ Veränderlichen, derjenigen Formen mit $n-1$ Veränderlichen nämlich, deren Determinante

$$(-1)^\tau d_{n-2} b$$

ist und welche eigentlich durch das Geschlecht von $f(x_\varrho)$ darstellbar sind. Diesem Geschlechte kämen folgende Charaktere zu: die Charaktere

$$\left(\frac{b_m}{p_m}\right) = \left(\frac{f'_m}{p_m}\right) \qquad (C')$$
$$(m = 1, 2, \cdots n-2)$$

bezüglich aller in o_m aufgehenden Primfaktoren p_m, und ausserdem die Charaktere

$$\left(\frac{b_{n-2}}{q}\right) = \left(\frac{(-1)^{\tau+1} \cdot o_{n-1}}{q}\right) \qquad (C'')$$

bezüglich aller in b aufgehenden ungeraden Primfaktoren q. Nennt man τ' den Index des Geschlechts $\Gamma_{(1)}$ und setzt

$$\psi'(o, n-2)$$

$$= \sum_{m=1}^{n-3} \frac{1}{4}(b_m - 1)(o_m + 1) + \frac{1}{4}(b_{n-2} - 1)(o_{n-2}\varepsilon b + 1)$$

$$+ \sum_{m=1}^{n-2} \frac{1}{4}(b_m - 1)(b_{m+1} - 1),$$

$$\Pi' = (-1)^{\left[\frac{\tau'}{2}\right] + \psi'(o, n-2)} \cdot \prod_{m=1}^{n-2} \left(\frac{b_m}{o_m}\right) \cdot \left(\frac{b_{n-2}}{b}\right),$$

so wäre

(76) $$\Pi' = 1$$

die Möglichkeitsbedingung, welche dem Geschlechte $\Gamma_{(1)}$ entspricht, und man beweist leicht die Gleichheit

(77) $$\Pi' = \Pi.$$

In der That, da die Zahlen $b_1, b_2, \cdots b_{n-2}$ und $(-1)^\tau b$ mit den Zahlen $f_1', f_2', \cdots f_{n-2}', f_{n-1}'$ übereinstimmen, da ferner

$$\left(\frac{b_{n-2}}{b}\right) = \left(\frac{(-1)^{\tau+1} o_{n-1}}{b}\right) = \left(\frac{(-1)^{\tau+1} o_{n-1}}{f_{n-1}'}\right),$$

nach dem verallgemeinerten Reciprocitätsgesetze also

$$\left(\frac{b_{n-2}}{b}\right) = \left(\frac{f_{n-1}'}{o_{n-1}}\right)$$

$$\cdot (-1)^{\frac{1}{4}(f_{n-1}' - 1)(o_{n-1} + 1) + \frac{1}{4}(f_{n-1}' - 1)((-1)^\tau - 1) + \frac{\varepsilon - 1}{2} \cdot \frac{(-1)^{\tau+1} - 1}{2}}$$

gesetzt werden darf, so ergiebt sich zunächst

$$\psi'(o, n-2)$$

$$\equiv \sum_{m=1}^{n-2} \frac{1}{4}(f_m' - 1)(o_m + 1) + \sum_{m=1}^{n-2} \frac{1}{4}(f_m' - 1)(f_{m+1}' - 1)$$
$$\pmod{2}$$

und sodann

$$\Pi' = \Pi \cdot (-1)^{\left[\frac{\tau}{2}\right] + \left[\frac{\tau'}{2}\right] + \frac{\varepsilon - 1}{2} \cdot \frac{(-1)^{\tau+1} - 1}{2}}.$$

Ist nun $\varepsilon = 1$ also $\tau' = \tau$, so ist $\Pi' = \Pi$. Ist dagegen $\varepsilon = -1$, so ist $\tau' = \tau - 1$; gleichviel aber, ob τ gerade oder ungerade ist, findet sich auch in diesem Falle

$$\Pi' = \Pi.$$

Andererseits, wenn das Geschlecht $\Gamma_{(I)}$ wirklich vorhanden ist, während b eine gegen 2Δ prime Zahl ist, die der Bedingungsgleichung (38) genügt, deren Charaktere bezüglich der Primzahlen p_{n-1} also mit den entsprechenden Charakteren (C) übereinstimmen, so erkennt man aus nr. 8 auch das Vorhandensein des Geschlechts G. Denn, ist dann $b(y_\varrho)$ eine beliebige Form des Geschlechts $\Gamma_{(I)}$, so folgt aus jener nr., dass es eine Form $g(y_\varrho)$ giebt, welche nach der über b gemachten Annahme dem vorgeschriebenen Geschlechte G angehört.

Hieraus ist zu schliessen: Werden die Charaktere (C) für Formen der Ordnung O ganz nach Belieben so gewählt, dass die Möglichkeitsbedingung (74) erfüllt wird, so werden die Charaktere (C'), (C'') für Formen mit $n-1$ Veränderlichen, der Gleichung (77) zufolge, auch der Möglichkeitsbedingung (76) Genüge leisten. Nimmt man daher als bereits bewiesen an, dass bei Formen mit $n-1$ Veränderlichen, deren Determinante ungerade und deren erste σ-Invariante gleich 1 ist, jedem Systeme von Einzelcharakteren, welches mit der Möglichkeitsbedingung verträglich ist, wirklich ein Geschlecht solcher Formen entspricht, so ist das Geschlecht $\Gamma_{(I)}$ wirklich vorhanden. Alsdann aber giebt es, wie zuletzt bemerkt, auch ein bestimmtes ihm entsprechendes Geschlecht G von Formen mit n Veränderlichen und den vorgeschriebenen Charakteren, d. h. es ist auch für Formen mit n Veränderlichen, deren Determinante ungerade und deren erste σ-Invariante gleich 1 ist, gezeigt, dass jedem mit der Möglichkeitsbedingung verträglichen Systeme von Einzelcharakteren ein wirkliches Geschlecht entspricht. Da dieser Umstand aber bei ternären Formen früher als zutreffend erkannt worden ist, steht er hiernach allgemein fest. —

Derselbe Satz gilt auch für den Fall einer geraden ersten σ-Invariante und ist auf ähnlichem Wege zu erweisen.

Zehntes Capitel.

Positive Formen. Vom Maasse derselben.

1. Von nun an setzen wir $\tau = 0$ d. h. die Formen mit n Veränderlichen, die wir untersuchen, als bestimmte und zwar positive Formen voraus. Da die Determinante immer von Null verschieden gedacht wird, lässt sich nach nr. 11 des fünften Capitels jede solche Form $f(x_\varrho)$, mit einer von Null verschiedenen ganzen Zahl M multiplicirt, auf die Gestalt bringen:

$$(1) \qquad M \cdot f(x_\varrho) = m_1 X_1^2 + m_2 X_2^2 + \cdots + m_n X_n^2,$$

in welcher $m_1, m_2, \cdots m_n$ positive ganze Zahlen und

$$X_1, X_2, \cdots X_n$$

homogene lineare Funktionen von $x_1, x_2, \cdots x_n$ mit ganzzahligen Coefficienten sind. Aus diesem Umstande ist bereits am Schlusse des fünften Capitels der Satz gewonnen, dass nur eine endliche Menge von Darstellungen einer Zahl m durch eine positive Form $f(x_\varrho)$ d. i. nur eine endliche Menge ganzzahliger Lösungen der Gleichung

$$(2) \qquad f(x_\varrho) = m$$

vorhanden ist. Hieraus folgt weiter: eine positive Form

$$f(x_\varrho) = \sum_1^n a_{i\varkappa} x_i x_\varkappa$$

besitzt nur eine endliche Anzahl ganzzahliger Transformationen in sich selbst. Denn, ist

$$(3) \qquad x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho n} y_n \quad (\varrho = 1, 2, \cdots n)$$

eine solche Transformation, so muss

$$f(q_{\varrho i}) = a_{ii}$$

sein, d. h. die Zahlen

$$q_{1i}, q_{2i}, \cdots q_{ni},$$

welche die i^{te} Spalte im Coefficientensysteme der Substitution (3) ausmachen, liefern eine Darstellung von a_{ii} durch die Form $f(x_\varrho)$.

Mithin lassen die Elemente jeder einzelnen Spalte in der Substitution (3) nur eine endliche Menge von Werthsystemen zu, und umsomehr kann die Anzahl der Substitutionen (3) selbst nur eine endliche sein, da jene Werthsysteme, um eine solche zu bilden, noch der Bedingung $|q_{i\varkappa}| = 1$ Genüge zu leisten haben.

Insbesondere ist für die Form

$$f(x_\varrho) = x_1^2 + x_2^2 + \cdots + x_n^2$$

die Anzahl ihrer Transformationen in sich selbst gleich

$$2^{n-1} \cdot 1 \cdot 2 \cdot 3 \cdots n.$$

In der That, wenn die Gleichungen (3) eine solche darstellen, so müssen die ganzen Zahlen $q_{i\varkappa}$ folgenden Bedingungen genügen:

(4a) $$q_{1i}^2 + q_{2i}^2 + \cdots + q_{ni}^2 = 1 \quad (i = 1, 2, \cdots n)$$

und

(4b) $$q_{1i}q_{1\varkappa} + q_{2i}q_{2\varkappa} + \cdots + q_{ni}q_{n\varkappa} = 0. \quad (i \gtrless \varkappa)$$

Die Bedingung (4a) erfordert zunächst, dass von den Zahlen $q_{1i}, q_{2i}, \cdots q_{ni}$ nur eine einzige, etwa q_{hi}, von Null verschieden, gleich ± 1 sei, in Folge davon zeigt dann (4b), dass $q_{h\varkappa}$ für jeden von i verschiedenen Werth $\varkappa$ gleich Null ist. Demnach ist in der Determinante $|q_{i\varkappa}|$ in jeder Spalte sowohl, wie in jeder Zeile nur ein einziges von Null verschiedenes Element und dieses muss ± 1 sein. Alle möglichen Fälle dieser Art werden offenbar erhalten, wenn man das von Null verschiedene Glied der ersten Zeile an irgend einer ihrer n Stellen wählt, dann das von Null verschiedene Glied der zweiten Zeile an irgend einer der übrigen $n - 1$, das der dritten Zeile dann an irgend einer der übrigen $n - 2$ Stellen u. s. w. Dies giebt $1 \cdot 2 \cdot 3 \cdots n$ verschiedene mögliche Fälle; in jedem von ihnen kann man jedes der von Null verschiedenen Glieder sowohl gleich $+1$ als gleich -1 wählen, ausgenommen das letzte, dessen Vorzeichen so gewählt werden muss, dass der Werth der Determinante $+1$ wird. So erhält man für jeden der möglichen Fälle 2^{n-1} Combinationen und folglich, wie be-

hauptet,

$$2^{n-1} \cdot 1 \cdot 2 \cdot 3 \cdots n$$

Transformationen der Form $f(x_\varrho)$ in sich selbst.

2. Die endliche Anzahl aller ganzzahligen Transformationen der beliebigen Form $f(x_\varrho)$ in sich selbst werde hinfort durch $t(f)$ bezeichnet. Für äquivalente Formen f und f_1 ist diese Anzahl dieselbe. Denn, verwandelt sich f in f_1 durch die Substitution S und folglich f_1 in f durch die inverse Substitution S^{-1} und ist F jede Transformation von f in sich selbst, so wird das Produkt $S^{-1}FS$ eine Substitution F_1 sein, durch welche f_1 in sich selbst übergeht, und alle solche Substitutionen liefern, die Anzahl der F_1 derjenigen der F also gleich sein.

Ist ferner $\mathfrak{f}$ die Reciproke von f, so besteht gleichfalls die Gleichheit

$$t(\mathfrak{f}) = t(f), \tag{5}$$

denn jeder Transformation von f in sich selbst entspricht nach nr. 7 des fünften Capitels eine Transformation von $\mathfrak{f}$ in sich selbst, und umgekehrt.

Nun werde der Werth $\frac{1}{t(f)}$ als *Maass* der Form $f(x_\varrho)$ definirt. Der voraufgeschickten Bemerkung zufolge wird das Maass einer Form zugleich das Maass jeder ihr äquivalenten Form sein und folglich auch als Maass ihrer Classe angesehen werden können. Man nenne ferner, wenn irgend ein Complex von Classen gegeben ist, die Summe ihrer Maasse das Maass ihres Complexes. Z. B. ist dann das Maass einer Ordnung oder eines Geschlechts von Formen die Summe der Maasse aller in dieser Ordnung resp. diesem Geschlechte enthaltenen Classen; sind also

$$f_1(x_\varrho),\ f_2(x_\varrho),\ \cdots \tag{6}$$

irgend welche Repräsentanten der Ordnung oder des Geschlechts, so wird die auf alle diese Repräsentanten erstreckte Summe

$$\sum_\varkappa \frac{1}{t(f_\varkappa)} \tag{7}$$

das Maass der Ordnung resp. des Geschlechts sein. Da

das reciproke Geschlecht durch die Reciproken der Formen repräsentirt werden kann, welche Repräsentanten des gegebenen Geschlechts sind, muss zufolge der Gleichung (5) das Maass eines Geschlechts stets demjenigen des reciproken Geschlechts gleich sein.

Wird ferner eine Zahl m durch die Form $f(x_\varrho)$ dargestellt, so soll das Maass der *Form* zugleich das Maass dieser *Darstellung* heissen. Ebenso, wenn m durch einen Complex mehrerer Formen oder mehrfach durch dieselbe Form dargestellt wird, soll das Maass dieses Complexes das Maass der verschiedenen Darstellungen von m heissen; gestattet also z. B. m durch die Repräsentanten (6) der Reihe nach $r_1, r_2, r_3, \cdots$ verschiedene Darstellungen, so wird $\sum_\varkappa \frac{r_\varkappa}{t(f_\varkappa)}$ das gesammte Maass dieser Darstellungen sein.

Wenn dagegen *eine Form mit $n-1$ Veränderlichen* durch *eine Form mit n Veränderlichen* dargestellt wird, so soll als das Maass dieser Darstellung das Produkt aus den Maassen beider Formen aufgefasst werden.

Man denke sich z. B. die sämmtlichen eigentlichen Darstellungen der im vorigen Capitel (s. nr. 10 desselben) mit b bezeichneten Zahl durch die Repräsentanten eines gegebenen Geschlechts $\mathfrak{G}$ von Formen mit n Veränderlichen, das dem Geschlechte G mit den Repräsentanten (6) reciprok ist. Zu diesem Zwecke bedarf man der Repräsentanten eines bestimmten Geschlechts $\Gamma_{(\mathrm{I})}$ (eventuell zweier bestimmten $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$) von (positiven) Formen mit $n-1$ Veränderlichen; ihre Anzahl sei γ. Jedem dieser γ Repräsentanten $b(y_\varrho)$ entsprechen, wenn β die Anzahl der Primfaktoren von b bezeichnet, 2^β Formen $g_i(y_\varrho)$ des Geschlechts G und jeder einzelnen von diesen entsprechend erhält man so viel verschiedene eigentliche Darstellungen von b durch eine der Formen

$$\mathfrak{f}_1(x_\varrho),\ \mathfrak{f}_2(x_\varrho),\ \cdots$$

etwa durch $\mathfrak{f}_\varkappa(x_\varrho)$, als die Menge aller Transformationen von $f_\varkappa(x_\varrho)$ in $g_i(y_\varrho)$, d. i. $t(f_\varkappa)$, getheilt durch die Menge aller Transformationen der Form $b(y_\varrho)$ in sich selbst, welche $t(b)$

heisse, beträgt, also

$$\frac{t(f_\varkappa)}{t(b)}.$$

Das Maass dieser eigentlichen Darstellungen von b ist mithin

$$\frac{t(f_\varkappa)}{t(b)} \cdot \frac{1}{t(f_\varkappa)} = \frac{1}{t(b)}$$

und folglich das Maass aller der eigentlichen Darstellungen von b, welche den sämmtlichen Formen $g_i(y_\varrho)$ entsprechen, gleich $\frac{2^\beta}{t(b)}$. Hieraus folgt für das Maass sämmtlicher eigentlichen Darstellungen von b durch die Repräsentanten des Geschlechts $\mathfrak{G}$ der Ausdruck

$$(8) \qquad 2^\beta \cdot \sum_b \frac{1}{t(b)},$$

wenn diese Summe auf sämmtliche γ Repräsentanten des Geschlechts $\Gamma_{(\mathrm{I})}$ (resp. der beiden Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$) erstreckt wird, d. i. kürzer, der Satz:

Das Maass sämmtlicher eigentlichen Darstellungen der Zahl b durch die Repräsentanten des Geschlechts $\mathfrak{G}$ von Formen mit n Veränderlichen ist gleich 2^β mal dem Maasse des Geschlechts $\Gamma_{(\mathrm{I})}$ (resp. der beiden Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$) von Formen mit $n-1$ Veränderlichen.

Da bezüglich jeder der 2^β Formen $g_i(y_\varrho)$ die Form $b(y_\varrho)$ so viel eigentliche Darstellungen durch eine Form $f_\varkappa(x_\varrho)$ des Geschlechts G besitzt, als diese Form Transformationen in sich selbst hat, also $t(f_\varkappa)$, zugleich aber der Bruch $\frac{1}{t(b)\,t(f_\varkappa)}$ das Maass jeder solchen Darstellung bezeichnet, so ist $\frac{1}{t(b)}$ das Maass dieser eigentlichen Darstellungen von $b(y_\varrho)$ durch $f_\varkappa(x_\varrho)$ und $2^\beta \cdot \frac{1}{t(b)}$ das Maass aller eigentlichen Darstellungen der Form $b(y_\varrho)$ durch die sämmtlichen Repräsentanten des Geschlechts G. Im Hinblick auf den Ausdruck (8) ergiebt sich folglich das Resultat:

Das Maass aller eigentlichen Darstellungen der *Zahl* b durch die Repräsentanten des Geschlechts $\mathfrak{G}$

ist zugleich das Maass aller eigentlichen Darstellungen der *Formen*, welche das Geschlecht $\Gamma_{(\mathrm{I})}$ (resp. die zwei Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$) repräsentiren, durch die Repräsentanten des Geschlechts G.

Wir haben in der Theorie der ternären Formen den einfachsten Fall des ersten dieser Sätze nach Gauss schon kennen gelernt. In der That bilden die positiven ternären Formen von der Ordnung $\begin{pmatrix}1, 1\\ 1, 1\end{pmatrix}$ nur eine einzige Classe, als deren Repräsentant die Form

$$x_1^2 + x_2^2 + x_3^2 \tag{9}$$

angesehen werden kann, sie bilden also auch nur ein einziges Geschlecht G. Da die Form (9) mit ihrer Reciproken identisch ist, so stimmt auch das reciproke Geschlecht $\mathfrak{G}$ mit G überein. Ist demnach b eine positive ungerade Zahl, welche > 1 gedacht werde (sonst aber keine Bedingung weiter zu erfüllen hat, da die Bedingungsgleichung (38) des vorigen Capitels ausfällt), so entspricht dem Geschlechte G ein bestimmtes Geschlecht $\Gamma_{(\mathrm{I})}$ eigentlich primitiver, eventuell auch ein Geschlecht $\Gamma_{(\mathrm{II})}$ uneigentlich primitiver positiver binärer Formen mit der Determinante b; letzteres jedoch fällt aus, sobald $b \equiv 1 \pmod{4}$ vorausgesetzt wird, da es uneigentlich-primitive binäre Formen mit einer solchen Determinante nicht giebt. Heisst demnach A die Anzahl aller eigentlichen Darstellungen von b durch die Form (9), sodass $\frac{A}{2^2 \cdot 1 \cdot 2 \cdot 3}$ das Maass derselben ist, so findet sich, da $t(b)$ für jede der binären Formen $b(y_\varrho)$ gleich 2 ist,

$$\frac{A}{24} = 2^\beta \cdot \frac{\gamma}{2} \text{ also } A = 3 \cdot 2^{\beta+2} \cdot \gamma;$$

γ bezeichnet die Classenzahl des Geschlechts $\Gamma_{(\mathrm{I})}$ oder auch des Haupt-Geschlechts eigentlich-primitiver Formen der Determinante b — wir erhalten also genau die Gauss'sche Formel (S. 139).

3. Als nächstes Beispiel werde auf gleiche Weise die Darstellung einer positiven ungeraden Zahl b durch eine Summe von vier Quadraten betrachtet. — Die quaternären Formen der Ordnung

$$\tau = 0, \begin{matrix} 1, & 1, & 1 \\ 1, & 1, & 1 \end{matrix}$$

bilden wieder*) nur eine einzige Classe, als deren Repräsentant die Form

(10) $$x_1^2 + x_2^2 + x_3^2 + x_4^2$$

betrachtet werden darf; sie bilden also auch nur ein einziges Geschlecht G, das mit seinem reciproken Geschlechte $\mathfrak{G}$ identisch ist; somit kann (10) auch als Repräsentant des letzteren angesehen werden. Ist nun b eine positive ungerade Zahl, so kommt, da n gerade ist, nur das Geschlecht $\Gamma_{(\mathrm{I})}$ der Ordnung $\begin{pmatrix} 1, & b \\ 1, & 1 \end{pmatrix}$ in Betracht. Die Charaktere (C'), (C'') — s. letzte nr. des vorigen Capitels — dieses ternären Geschlechts reduciren sich auf die Werthe des Ausdrucks $\left(\frac{b_2}{q}\right) = \left(\frac{-1}{q}\right)$ für die in b aufgehenden Primfaktoren q, wo $b_2 = \beta_{3,3}$ eine durch die Reciproke $\beta(y_\varrho)$ von $b(y_\varrho)$ darstellbare Zahl ist. Wendet man also zur Bestimmung des Maasses M dieses ternären Geschlechts die Eisenstein'sche Formel an**), so ist in letzterer $\varkappa = \beta$, $\lambda = 0$,

$$E = (-1)^{\frac{b+1}{2}} \cdot \left(\frac{b_2}{b}\right) = (-1)^{\frac{b+1}{2}} \cdot \left(\frac{-1}{b}\right) = -1$$

zu setzen, die auf die Buchstaben r und ω bezüglichen Produkte in derselben fallen aus und man erhält

(11) $$\mathsf{M} = \frac{b}{24 \cdot 2^\beta} \cdot \prod \left(1 + \frac{1}{q}\right).$$

Ist nun wieder A die Anzahl aller eigentlichen Darstellungen der Zahl b durch die Form (10), so ist ihr Maass gleich A dividirt durch die Anzahl der Transformationen, welche (10) in sich selbst verwandeln, d. i. durch

$$2^3 \cdot 1 \cdot 2 \cdot 3 \cdot 4 = 8 \cdot 24.$$

Dem Satze der vorigen nr. zufolge ist andererseits dieses Maass gleich $2^\beta \cdot \mathsf{M}$ und somit wird, wenn, in Primzahlpotenzen zerlegt,

---

*) S. Abschnitt III.

**) S. Seite 191.

(12) $$b = q_1^{h_1} \cdot q_2^{h_2} \cdots$$

ist, die Anzahl A der eigentlichen Darstellungen der positiven ungeraden Zahl b als Summe von vier Quadraten

(13) $$A = 8(q_1^{h_1} + q_1^{h_1-1})(q_2^{h_2} + q_2^{h_2-1}) \cdots.$$

Diese Formel ist auf arithmetischem Wege, der, wie man sich leicht überzeugt, mit dem hier dargestellten durchaus gleichbedeutend ist, zuerst von Eisenstein hergeleitet worden*). Es giebt ähnliche Formeln auch für den Fall, dass die dargestellte Zahl gerade ist, und sie können in analoger Weise hergeleitet werden, doch bedarf es dazu einer Erweiterung der hier gegebenen Grundlage.

Die Anzahl der eigentlichen Darstellungen ist für eine Zahl $2b$ dreimal, für eine Zahl $4b$ zweimal so gross wie zuvor, während man sogleich erkennt, dass eine durch 8 theilbare Zahl keine eigentliche Darstellung als Summe von vier Quadraten zulässt, da letztere, wenn sie nicht sämmtlich ungerade sind also eine Summe $\equiv 4 \pmod{8}$ geben, zu je zweien gerade und ungerade sein, also eine Summe $\equiv 2$ oder $6 \pmod{8}$ geben müssten.

Will man auch die uneigentlichen Darstellungen von b in Betracht ziehen, so muss man die eigentlichen Darstellungen aller Zahlen zählen, welche aus b durch Division mit einer Quadratzahl hervorgehen, also die Form haben:

$$b' = q_1^{h_1 - 2g_1} \cdot q_2^{h_2 - 2g_2} \cdots,$$

wo g_1 jeden der Werthe $0, 1, 2, \cdots \left[\frac{h_1}{2}\right]$; g_2 jeden der Werthe $0, 1, 2, \cdots \left[\frac{h_2}{2}\right]$ u. s. w. haben kann. Die Anzahl der eigentlichen Darstellungen dieser Zahl b' wäre

$$A' = 8 \cdot (q_1^{h_1-2g_1} + q_1^{h_1-2g_1-1})(q_2^{h_2-2g_2} + q_2^{h_2-2g_2-1}) \cdots,$$

wo jedoch, falls z. B. h_1 eine gerade Zahl ist, für den Werth $g_1 = \left[\frac{h_1}{2}\right]$ der entsprechende Faktor gleich 1 zu setzen ist, da

*) Eisenstein in dem Aufsatze: über die Vergleichung von solchen ternären quadratischen Formen, welche verschiedene Determinante haben.

für diesen Werth von g_1 die Zahl b' den Primfaktor q_1 nicht mehr enthält. Offenbar ist sonach A' nichts anderes als das allgemeine Glied in der Entwickelung des Produktes

$$\begin{aligned} 8 \cdot ((q_1^{h_1} + q_1^{h_1-1}) + (q_1^{h_1-2} + q_1^{h_1-3}) + \cdots + 1) \\ \cdot ((q_2^{h_2} + q_2^{h_2-1}) + (q_2^{h_2-2} + q_2^{h_2-3}) + \cdots + 1) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

und folglich ist die Summe aller A', bezogen auf die sämmtlichen Zahlen b' einschliesslich der Zahl b selbst, gleich diesem Produkte d. i. einfacher gleich

$$8 \cdot \prod_q \frac{q^{h+1} - 1}{q - 1}.$$

Oder: Die Anzahl aller (eigentlichen und uneigentlichen) Darstellungen einer ungeraden Zahl als Summe von vier Quadraten ist gleich der 8-fachen Summe aller ihrer Theiler*).

Jede gerade Zahl N kann gleich $2^{2\varkappa} \cdot b$ oder gleich $2^{2\varkappa} \cdot 2b$ gesetzt werden, wo b ungerade ist. Um ihre sämmtlichen eigentlichen oder uneigentlichen Darstellungen zu zählen, muss man die eigentlichen Darstellungen aller derjenigen Zahlen abzählen, welche aus N durch Division mit einem quadratischen Theiler entstehen. Ist zunächst $N = 2^{2\varkappa} \cdot b$, so erhält man auf solche Weise die Zahlen $2^{2h} \cdot b'$, wo $h \overline{\gtrless} \varkappa$; von diesen sind aber nur die Zahlen b' und $4b'$ eigentlicher Darstellungen fähig, deren Anzahl für jene gleich A', für diese $2A'$, zusammen also $3A'$ beträgt. Die Anzahl sämmtlicher Darstellungen von N ist mithin $3 \cdot \sum A'$. Ist zweitens $N = 2^{2\varkappa} \cdot 2b$, so sind nur diejenigen auf die gedachte Weise aus N entstehenden Zahlen, welche die Form $2b'$ haben, eigentlich darstellbar und zwar auf $3A'$ verschiedene Arten, also ist auch jetzt die Anzahl aller Darstellungen gleich $3 \sum A'$.

Man findet mithin diesen Satz, welcher dem vorigen ergänzend zur Seite tritt: Die Anzahl aller (eigentlichen

*) Ueber eine andere Herleitung dieser Formel nach Hermite (J. f. M. 47 sur la théorie des formes quadratiques, Second Mémoire, am Schlusse) s. Abschnitt III.

und uneigentlichen) Darstellungen einer geraden Zahl als Summe von vier Quadraten ist gleich der 24fachen Summe aller ihrer ungeraden Theiler. Man findet in Eisenstein's Abhandlung „Neue Theoreme der höheren Arithmetik" eine Reihe von Sätzen derselben Art, welche sich auf die Darstellung durch andere einfache quaternäre Formen beziehen; sie können sämmtlich aus denselben Principien gewonnen werden, wie der soeben ausführlich hergeleitete Satz*).

4. Schon vor Eisenstein hat Jacobi aus der Theorie der elliptischen Funktionen, nämlich durch Vergleichung der Formel (35) S. 106 und (7) S. 184 seiner fundamenta nova theor. funct. ellipticarum den Satz gewonnen, der als einfacher Fall in dem angeführten enthalten ist: Das Vierfache $4m$ jeder positiven ungeraden Zahl gestattet soviel Darstellungen in der Form

$$t^2 + u^2 + v^2 + w^2$$

mittels positiver ungerader Zahlen t, u, v, w, als die Summe der Theiler von m beträgt. Später gab er (Crelle's J. f. M. 12 S. 167; vgl. Bd. 3) einen elementaren Beweis dieses Satzes, der, wie Dirichlet sich ausdrückt**), eine Uebertragung der Umformungen ist, welche Jacobi, um den Satz zu finden, mit seinen Reihen vornehmen musste. Dirichlet selbst hat, indem er sich vorbehielt, den Satz im Zusammenhange einer allgemeineren Theorie, die leider nicht

*) Liouville hat in seinem Journal 2. sér. t. 5 und 6 für die Anzahl der Darstellungen von Zahlen durch einige andere quaternäre Formen von einfacher Gestalt (ohne Beweis) Formeln mitgetheilt:

t. 5 p. 147	für die Form	$x^2 + y^2 + 3(z^2 + t^2)$
t. 5 p. 269	„ „ „	$x^2 + y^2 + 2(z^2 + t^2)$
t. 5 p. 305	„ „ „	$x^2 + y^2 + 4(z^2 + t^2)$
t. 6 p. 225	„ „ „	$x^2 + y^2 + z^2 + 2t^2$ und $x^2 + 2(y^2 + z^2 + t^2)$
t. 6 p. 324	„ „ „	$x^2 + y^2 + z^2 + 8t^2$ und $x^2 + 2y^2 + 4z^2 + 8t^2$.

S. bezüglich des Beweises derselben eine Arbeit von Pepin in Liouv. J. des Math. 4. sér. t. 6, sur quelques formes quadratiques quaternaires.

**) S. Liouville's J. des Math. 2. série, t. 1, p. 210—215.

mehr von ihm veröffentlicht worden ist, herzuleiten, wenigstens dem Jacobi'schen Beweise eine classische Darstellung gewidmet, welche seine arithmetisch-algebraische Grundlage ins hellste Licht setzt, und die wir uns nicht versagen können, hier aufzunehmen.

Vor allem bemerke man, dass die ungeraden Lösungen der Gleichung

$$(14) \qquad 4m = t^2 + u^2 + v^2 + w^2$$

offenbar sämmtlich gefunden werden, wenn man auf alle Weise $2m$ durch die Formel

$$(15) \qquad 2m = p + q$$

in zwei positive ungerade Summanden zerlegt und dann die Gleichungen löst

$$(16) \qquad 2p = t^2 + u^2, \quad 2q = v^2 + w^2.$$

Nun folgt aus allgemeineren Sätzen der Lehre von den binären quadratischen Formen*), dass die Anzahl der Lösungen der Gleichung $2p = t^2 + u^2$ dem Ueberschusse der Anzahl derjenigen Zerlegungen $p = ad$ in zwei positive Faktoren, bei denen $a \equiv 1 \pmod{4}$, über die Anzahl derjenigen, bei denen $a \equiv 3$ ist, gleich ist. Giebt man also je nach diesen Fällen dem Zeichen δ den Werth $+1$ oder -1, so ist $\sum \delta$ die Anzahl Lösungen der ersten der Gleichungen (16), und ebenso $\sum \varepsilon$ die Anzahl Lösungen der zweiten von ihnen, wenn $\varepsilon = +1$ oder -1 gesetzt wird, jenachdem in der Zerlegung $q = bc$ der Faktor $b \equiv 1$ oder $\equiv 3 \pmod{4}$ ist; die Summen sind auf die bezeichneten Zerlegungen zu erstrecken.

Das entwickelte Produkt

$$\sum \delta \cdot \sum \varepsilon = \sum \eta$$

wird offenbar eine Summe von Einheiten η sein, welche $+1$ oder -1 sind, jenachdem $a - b$ theilbar oder nicht theilbar ist durch 4, oder auch — da man unschwer erkennt, dass von den beiden Zahlen $a - b$, $c + d$ stets eine aber auch nur eine durch 4 aufgeht — jenachdem $c + d$ nicht theilbar oder theil-

*) S. Analytische Zahlentheorie S. 114.

bar ist durch 4. Nun giebt jenes Produkt die Anzahl Lösungen der Gleichung (14), welche einer bestimmten Zerlegung (15) von $2m$ entsprechen. Die gesammte Summe

$$\sum \eta,$$

gebildet für alle verschiedenen Zerlegungen

$$(17) \qquad 2m = ad + bc,$$

wird demnach die Anzahl sämmtlicher Lösungen der Gleichung (14) in positiven ungeraden Zahlen t, u, v, w repräsentiren.

Die Zerlegungen (17) können in zwei Arten unterschieden werden: in solche, bei denen $a = b$, und solche, wo sie verschieden von einander sind. Offenbar kann man in Folge davon

$$\sum \eta = \sum \eta' + 2 \sum \eta''$$

setzen, indem man die erste Summe auf die Zerlegungen der ersten Art, die zweite auf diejenigen der zweiten Art erstreckt, in denen etwa $a > b$ ist.

Dies vorausgeschickt, führen wir durch die Gleichungen

$$(18) \qquad \begin{cases} a' = c(x+1) + d(x+2) \\ b' = cx + d(x+1) \\ c' = a(x+1) - b(x+2) \\ d' = -ax + b(x+1), \end{cases}$$

in welchen x ganzzahlig gedacht wird, neben den positiven ungeraden Zahlen a, b, c, d vier andere offenbar ungerade Zahlen a', b', c', d' ein, von denen sogleich einleuchtet, dass

$$(19) \qquad a'd' + b'c' = ad + bc$$

ist. Sollen sie aber auch positiv sein, so folgt aus den Beziehungen

$$c' = (a-b)(x+1) - b, \; d' = b - (a-b)x,$$

dass $(a-b)x$ dasjenige Vielfache der geraden Zahl $a-b$ sein müsse, das unmittelbar unter b liegt; für x darf dann also nur ein einziger bestimmter Werth gewählt werden, der Null oder positiv ist also auch a', b' zu positiven Zahlen macht, während noch

$$(20) \qquad a' - b' = c + d$$

also $a' > b'$ ist. Aus dieser Betrachtung geht hervor, dass jeder Zerlegung

$$2m = ad + bc$$

der zweiten Art durch die Gleichungen (18) eine ganz bestimmte Zerlegung derselben Art zugeordnet ist, die von der ersteren verschieden sein muss, weil sonst $a - b = c + d$ wäre, was einer zuvor gemachten Bemerkung zufolge unmöglich ist. Geht man nun auf dieselbe Weise von a', b', c', d' aus mittels der Gleichungen

$$(21) \qquad \begin{cases} a'' = c'(x' + 1) + d'(x' + 2) \\ b'' = c'x' + d'(x' + 1) \\ c'' = a'(x' + 1) - b'(x' + 2) \\ d'' = - a'x' + b'(x' + 1) \end{cases}$$

zu einer neuen Zerlegung über, so ist, wie bemerkt, der hierzu dienende Werth von x' nur ein einziger. Da man aber durch Auflösung der Gleichungen (18)

$$\begin{aligned} a &= c'(x + 1) + d'(x + 2) \\ b &= c'x + d'(x + 1) \\ c &= a'(x + 1) - b'(x + 2) \\ d &= - a'x + b'(x + 1) \end{aligned}$$

findet, die Formeln (21) also für $x' = x$ Zahlen

$$a'' = a, \; b'' = b, \; c'' = c, \; d'' = d$$

der gesuchten Art liefern, so erkennt man, dass der Zerlegung a', b', c', d' wieder die ursprüngliche Zerlegung a, b, c, d zugeordnet ist.

Demnach setzt sich $\sum \eta''$ aus Paaren von Einheiten zusammen, von denen die eine der Zerlegung

$$2m = ad + bc,$$

die andere der Zerlegung

$$2m = a'd' + b'c'$$

entspricht; diese jedoch sind der Beziehung (20) wegen einander entgegengesetzt und folglich

$$\sum \eta'' = 0.$$

Man erhält daher

$$\sum \eta = \sum \eta',$$

wo jede Einheit η' wegen $a = b$ eine positive ist, $\sum \eta$ ist also gleich der Anzahl der Zerlegungen

$$2m = a(d + c). \tag{22}$$

Hier bedeutet die ungerade Zahl a irgend einen Theiler von m, daher $d + c$ jede Zerlegung von $\frac{2m}{a}$ in zwei ungerade Summanden; da es solcher Zerlegungen $\frac{m}{a}$ giebt, ist die Anzahl jener Zerlegungen (22) gleich der Summe aller Zahlen $\frac{m}{a}$ d. i. gleich der Summe aller Theiler von m, w. z. b. w.

5. Der Fall, welcher sich nun zuerst darbietet, wenn man diesen Betrachtungen weiter nachgeht, ist die Darstellung einer positiven ungeraden Zahl b als Summe von fünf Quadraten oder durch die Form

$$f(x_\varrho) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2. \tag{23}$$

Auch hier wieder kann diese Form als Repräsentant der einzigen Classe sowie des einzigen Geschlechts G von Formen angesehen werden, welche in der Ordnung

$$\tau = 0, \begin{matrix} 1, & 1, & 1, & 1 \\ 1, & 1, & 1, & 1 \end{matrix}$$

vorhanden sind*). Die Reciproke der Form (23) ist ihr wiederum gleich, und somit diese Form auch Repräsentant des reciproken Geschlechts $\mathfrak{G}$. Die ungerade Zahl ist keinen Bedingungen zu unterwerfen, da die Bedingung (38) vorigen Capitels von selbst erfüllt ist. Ist sie beliebig gewählt, so kommen bezüglich ihrer Darstellungen durch die Form (23) die Geschlechter $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$ der beiden Ordnungen

$$\begin{matrix} 1, & 1, & b \\ 1, & 1, & 1 \end{matrix} \quad \text{und} \quad \begin{matrix} 1, & 1, & b \\ 2, & 1, & 2 \end{matrix}$$

in Betracht. Das erstere ist stets vorhanden (s. nr. 11

*) S. Abschnitt III.

des vorigen Capitels), das letztere jedoch, wie vor allem gezeigt werden muss, nur dann, wenn b von der Form $8n+5$ ist. In der That darf man die mit $b(y_\varrho)$ bezeichnete Form als charakteristische Form (mod. $8b\Delta$) ihrer Classe vorstellen, sodass, wenn sie der zweiten Ordnung angehört, sie einer Congruenz von der Gestalt

$$(24) \qquad b(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0, & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0, & 0 \\ 0 & 0 & 2a', & \mathfrak{A}' \\ 0 & 0 & \mathfrak{A}', & 2\mathfrak{a}' \end{Bmatrix} \pmod{8}$$

und folglich die entsprechende Form $g(y_\varrho)$ der Congruenz

$$g(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0, & 0, & b_{15} \\ \mathfrak{A}, & 2\mathfrak{a}, & 0, & 0, & b_{25} \\ 0 & 0 & 2a', & \mathfrak{A}', & b_{35} \\ 0 & 0 & \mathfrak{A}', & 2\mathfrak{a}', & b_{45} \\ b_{15} & b_{25} & b_{35} & b_{45} & b_{55} \end{Bmatrix} \pmod{8}$$

genügen würde. Man sieht hieraus, wie in nr. 7 des vorigen Capitels, dass $g(y_\varrho)$ einer Form $g'(y_\varrho)$ äquivalent ist, für welche

$$g'(y_\varrho) \equiv \begin{Bmatrix} 2a, & \mathfrak{A}, & 0, & 0, & 0 \\ \mathfrak{A}, & 2\mathfrak{a}, & 0, & 0, & 0 \\ 0 & 0 & 2a', & \mathfrak{A}', & 0 \\ 0 & 0 & \mathfrak{A}', & 2\mathfrak{a}', & 0 \\ 0 & 0 & 0 & 0 & \mathfrak{b} \end{Bmatrix} \pmod{8}$$

ist. Da diese Form der Form (23) äquivalent sein muss, ist ihre Determinante und demnach $\mathfrak{b}$ ungerade; ferner giebt es eine Substitution

$$x_\varrho = q_{\varrho 1} y_1 + q_{\varrho 2} y_2 + \cdots + q_{\varrho 5} y_5,$$
$$(\varrho = 1, 2, 3, 4, 5)$$

durch welche $f(x_\varrho)$ in $g'(y_\varrho)$ übergeht, sodass folgende Congruenzen erfüllt sind:

$$q_{1i}q_{15} + q_{2i}q_{25} + \cdots + q_{5i}q_{55} \equiv 0$$

$$q_{1i}^2 + q_{2i}^2 + \cdots + q_{5i}^2 \equiv 0$$

also auch

$$q_{1i} + q_{2i} + \cdots + q_{5i} \equiv 0$$

und

$$q_{1i}(q_{15} - 1) + q_{2i}(q_{25} - 1) + \cdots + q_{5i}(q_{55} - 1) \equiv 0 \pmod{2},$$
$$(i = 1, 2, 3, 4)$$

Congruenzen, denen man als fünfte die selbstverständliche

$$q_{15}(q_{15} - 1) + q_{25}(q_{25} - 1) + \cdots + q_{55}(q_{55} - 1) \equiv 0 \pmod{2}$$

hinzufügen kann und aus denen, da $|q_{i\varkappa}| = 1$ ist, hervorgeht, dass $q_{15}, q_{25}, \cdots q_{55}$ sämmtlich ungerade sein müssen. Da aber

$$q_{15}^2 + q_{25}^2 + \cdots + q_{55}^2 \equiv \mathfrak{b} \pmod{8}$$

ist, muss $\mathfrak{b} \equiv 5 \pmod{8}$ und wegen der Beziehungen

$$\varDelta = 1, \ \mathsf{B} = b, \ \varDelta \equiv \mathsf{B} \cdot \mathfrak{b} \pmod{8}$$

auch $b \equiv 5 \pmod{8}$ sein. — **Dass diese Bedingung aber für die Existenz des Geschlechtes $\Gamma_{(\mathrm{II})}$ auch ausreichend ist, ersieht man daraus, dass alsdann die Möglichkeitsbedingung**

$$(25) \qquad (-1)^{\left[\frac{\tau'}{2}\right]} \cdot (-1)^{\psi'(o,3)} \cdot \left(\frac{b_2}{b}\right) = 1$$

erfüllt ist. In der That ist $\tau' = \tau = 0$, ferner wegen (57') und (58) vorigen Capitels

$$\left(\frac{2b_3}{b}\right) = \left(\frac{(-1)^{\tau+1} o_4}{b}\right) = \left(\frac{-1}{b}\right)$$

d. i.

$$\left(\frac{b_3}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{b^2-1}{8}} = -1,$$

endlich

$$\psi'(o, 3) = \frac{1}{2}(b_1 - 1) + \frac{1}{2}(b_2 - 1) + \frac{1}{4}(b_3 - 1)(b + 1)$$
$$+ \frac{1}{4}(b_1 - 1)(b_2 - 1)$$
$$+ \frac{1}{4}(b_2 - 1)(b_3 - 1);$$

aus (24) aber folgt $b_2 \equiv -1 \pmod{4}$, daher wird, wenn $b \equiv 5 \pmod{8}$ vorausgesetzt wird,

$$\psi'(o, 3) \equiv 1 \pmod{2}$$

also die Gleichheit (25) erfüllt.

Nennen wir nun M_I und M_{II} die Maasse der beiden Geschlechter $\Gamma_{(I)}$ und $\Gamma_{(II)}$ und A die Anzahl aller eigentlichen Darstellungen von b durch die Form (23), so ist, da die Menge der Transformationen der Form in sich selbst

$$2^4 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 1920$$

beträgt, das Maass jener Darstellungen einerseits gleich $\frac{A}{1920}$, andererseits gleich $2^{\beta} \cdot M_I$ resp. gleich $2^{\beta} \cdot (M_I + M_{II})$, jenachdem b von einer der drei Formen $8n + 1, 3, 7$ oder von der Form $8n + 5$ ist. Man findet also je nach diesen beiden Fällen

$$(26) \qquad A = 1920 \cdot 2^{\beta} \cdot M_I \quad \text{oder} \quad 1920 \cdot 2^{\beta} \cdot (M_I + M_{II}).$$

6. Alles kommt darauf an, die Maasse M_I resp. M_{II} zu bestimmen.

Wir suchen zuerst M_I. Es handelt sich dabei um dasjenige Geschlecht der Ordnung

$$(O) \qquad \begin{pmatrix} 1, & 1, & b \\ 1, & 1, & 1 \end{pmatrix},$$

dessen Repräsentanten $b(y_{\varrho})$, die als charakteristische Formen (mod. $2b\Delta$) gedacht werden dürfen, die auf die verschiedenen Primfaktoren q von b bezüglichen Einzelcharaktere

$$(27) \qquad \left(\frac{b_3}{q}\right) = \left(\frac{-o_4}{q}\right) = \left(\frac{-1}{q}\right)$$

haben. Das Maass eines jeden quaternären Geschlechts hat Smith in seiner Arbeit über die Darstellung einer Zahl als Summe von fünf Quadraten durch völlig analoge Betrachtungen bestimmt, als sie zur Ableitung des Maasses ternärer Formen nach seinem Vorgange von uns angewandt worden sind. Grösserer Einfachheit sowohl als grösserer Mannigfaltigkeit wegen ziehen wir hier jedoch vor, die Methode zu befolgen, welche zu gleichem Zwecke Minkowski verwendet hat und welche sich an die Art anschliesst, wie Dirichlet die Anzahl der Geschlechter binärer Formen bestimmt hat.

Wir schicken dieser Untersuchung eine Hilfsformel voraus. — Seien $\psi(m)$ und $\Psi(m)$ zwei zahlentheoretische Funktionen, welche, während p jede Primzahl, m, m_0

aber irgend welche positive Zahlen bedeuten, die zu einer gegebenen Zahl N prim sind, folgenden Bedingungen Genüge leisten:

$$\psi(mm_0) = \psi(m)\psi(m_0), \quad \psi(p) \text{ num.} \overline{\gtrless} 1, \quad \psi(1) = 1$$

$$\Psi(mm_0) = \Psi(m)\Psi(m_0), \quad \Psi(p) = \pm \frac{1}{p^{1+2\varrho}}, \quad \Psi(1) = 1.$$

Das Produkt

$$(28) \qquad \prod_p \Big(1 + (1+\psi(p))\Psi(p) + (1+\psi(p))\Psi(p^2) + \cdots\Big)$$

werde auf alle in N nicht enthaltenen Primzahlen p bezogen. Da man wegen $\Psi(p^x) = \Psi(p)^x$ seinem allgemeinen Gliede den Ausdruck

$$\frac{1-(\psi(p)\Psi(p))^2}{(1-\Psi(p))(1-\psi(p)\Psi(p))}$$

geben kann, lässt es sich in folgender Form darstellen:

$$\frac{\prod \frac{1}{1-\Psi(p)} \cdot \prod \frac{1}{1-\psi(p)\Psi(p)}}{\prod \frac{1}{1-(\psi(p)\Psi(p))^2}},$$

wo man nun, so lange $\varrho > 0$ ist, die Produkte durch convergente Reihen ersetzen und, indem man jede der Summationen auf alle positiven gegen N primen Zahlen m erstreckt, schreiben darf:

$$(28\text{a}) \qquad \frac{\sum \Psi(m) \cdot \sum \psi(m)\Psi(m)}{\sum \psi(m)^2 \cdot \Psi(m)^2}.$$

Führt man andererseits in (28) die Multiplikation aus, so wird das allgemeine Glied der Entwickelung

$$\prod (1+\psi(p)) \cdot \Psi(m)$$

sein, wenn unter m wieder jede gegen N prime positive Zahl verstanden, die Multiplikation im ersten Faktor aber auf alle Primfaktoren von m erstreckt wird. Somit geht durch Vergleichung der beiden Ausdrücke (28), (28a) die Gleichung

$$(29) \qquad \sum_m \Big(\prod (1+\psi(p)) \cdot \Psi(m)\Big) = \frac{\sum\limits_m \Psi(m) \cdot \sum\limits_m \psi(m)\Psi(m)}{\sum\limits_m \psi(m)^2 \cdot \Psi(m)^2}$$

hervor, welches die gedachte Hilfsformel ist.

betrachte nun sämmtliche Classen der Ordnung (O) diese durch irgend welche (mod. $2b\Delta$) charakte-nen $b(y_\varrho)$ repräsentirt. Das Geschlecht jedes anten $b(y_\varrho)$ wird, wenn $q_1, q_2, \cdots q_\beta$ die ver-hlen sind, aus denen b besteht, durch die -1 charakterisirt, welche den Einzel-

$$\left(\frac{b_3}{q_2}\right), \cdots \left(\frac{b_3}{q_\beta}\right)$$

e durch die Reciproke $\beta(y_\varrho)$ von Zahl bedeutet, den Symbolen

$$\left(\frac{m}{q_\gamma}\right)$$

n Combinationen dieser hnen entspricht auch g (O). Zum Beweise dient liebige Wahl der Combination keitsbedingung, d. i. im vorliegenden eichung

$$(-1)^{\psi'(o,3)} \cdot \left(\frac{b_3}{b}\right) = 1$$

beschränkt ist; da aber neben den Hauptcharakteren (30) keine supplementären vorhanden sind, kann man $\psi'(o, 3)$ (mod. 2) beliebig und folglich auch so wählen, dass, nachdem für die Charaktere (30) beliebig genommen wurden, die Werthe die Gleichung erfüllt ist. Somit zerfällt die Ordnung (O) in 2^β wirklich vorhandene Geschlechter; $\Gamma_{(I)}$ ist von ihnen dasjenige, für welches die Werthe der Charaktere (30) durch die Formel (27) bestimmt sind; diese so bestimmten, dem Geschlechte $\Gamma_{(I)}$ charakteristischen Werthe der Charaktere (30) seien

$$(32) \qquad \varepsilon_1, \varepsilon_2, \cdots \varepsilon_\gamma.$$

Man setze alsdann

$$\varpi(b) = \left(1 + \varepsilon_1 \cdot \left(\frac{b_3}{q_1}\right)\right)\left(1 + \varepsilon_2 \cdot \left(\frac{b_3}{q_2}\right)\right) \cdots \left(1 + \varepsilon_\gamma \cdot \left(\frac{b_3}{q_\beta}\right)\right)$$

und betrachte folgende Summe:

$$(33) \qquad S = \sum_b \left(\frac{\varpi(b)}{t(b)} \cdot \lim_{\varrho=0} . \varrho \sum \frac{1}{\beta(y_\varrho)^{2+2\varrho}} \right),$$

in welchem Ausdrucke die äussere Summation auf sämmtliche Repräsentanten $b(y_\varrho)$ der Ordnung (O), die innere jedoch, bei welcher $\beta(y_\varrho)$ die Reciproke des jedesmaligen Repräsentanten bedeutet, auf alle ganzzahligen Werthsysteme

$$y_1, y_2, y_3, y_4$$

ohne gemeinsamen Theiler bezogen werden soll, für welche $\beta(y_\varrho)$ prim wird gegen $2b$. Zunächst geht nun aus einer allgemeinen Formel, die später bewiesen werden soll*), hervor, dass die letztere Summe für ein gegen Null convergirendes ϱ einen von der speciellen Form $\beta(y_\varrho)$ unabhängigen festen Grenzwerth hat:

$$(34) \qquad \lim_{\varrho=0} . \varrho \sum \frac{1}{\beta(y_\varrho)^{2+2\varrho}} = L,$$

wo

$$(34a) \qquad L = \frac{4\pi^2}{15 S_4} \cdot \prod_q \frac{1-\frac{1}{q}}{1-\frac{1}{q^4}} \cdot \frac{1}{b^{3/2}}$$

und

$$S_4 = \sum_{s=1}^{\infty} \frac{1}{s^4}$$

zu setzen ist, während die Multiplikation sich auf alle Primfaktoren q von b bezieht. Da andererseits $\varpi(b)$ verschwindet, sobald irgend eins der Symbole (30) einen von der entsprechenden Einheit (32) verschiedenen Werth hat, die Form $b(y_\varrho)$ also einem von $\Gamma_{(\mathrm{I})}$ verschiedenen Geschlecht angehört, dagegen $\varpi(b) = 2^\beta$ wird, wenn sämmtliche Symbole (30) den entsprechenden Einheiten (32) gleich sind, also $b(y_\varrho)$ eine Form des Geschlechts $\Gamma_{(\mathrm{I})}$ ist, so findet sich offenbar aus (33) einfacher:

$$(35) \qquad S = 2^\beta \cdot \mathsf{M}_{\mathrm{I}} \cdot L.$$

7. Andererseits kann man die Summe S, da sie, so lange $\varrho > 0$, nach Dirichlet'schen Sätzen absolut convergent ist,

*) Siehe nr. 10 Anmerkung.

nach den wachsenden Werthen ordnen, welche die Formen $\beta(y_\varrho)$ darin erhalten. Diese Werthe sind die sämmtlichen positiven zu $2b$ primen ganzen Zahlen. In der That erhalten die Formen $\beta(y_\varrho)$ bei der Summation (33) nur solche Werthe; um aber sich zu überzeugen, dass auch jede solche Zahl m durch eine der Formen $\beta(y_\varrho)$ dargestellt erscheinen muss, bedenke man, dass die Charaktere

$$\left(\frac{m}{q_1}\right), \left(\frac{m}{q_2}\right), \cdots \left(\frac{m}{q_\beta}\right)$$

nothwendig mit den Einzelcharakteren eines bestimmten Geschlechts der Ordnung (O) übereinstimmen müssen; diesem Geschlechte von Formen mit 4 Veränderlichen — es heisse G' — entspricht ein bestimmtes Geschlecht $\Gamma'_{(1)}$ von ternären Formen mit der Determinante m, welche durch dasselbe eigentlich darstellbar sind, auch ist es nach nr. 11 des vorigen Capitels ein wirkliches, für das also thatsächlich Repräsentanten vorhanden sind, und somit muss nach nr. 10 des vorigen Capitels m durch einen der Repräsentanten $\beta(y_\varrho)$ des zu G' reciproken Geschlechts eigentlich darstellbar sein. Denken wir uns demnach die Summe S nach den wachsenden Werthen m welche positiv und gegen $2b$ prim sind, geordnet. Da ihr allgemeines Glied auch folgendermassen geschrieben werden kann:

$$\frac{1}{t(b)} \cdot \frac{\varpi(m)}{\beta(y_\varrho)^{2+2\varrho}} = \frac{1}{t(b)} \cdot \frac{\varpi(m)}{m^{2+2\varrho}},$$

wenn m die durch $\beta(y_\varrho)$ dargestellte Zahl ist und

$$\varpi(m) = \left(1 + \varepsilon_1 \cdot \left(\frac{m}{q_1}\right)\right)\left(1 + \varepsilon_2 \cdot \left(\frac{m}{q_2}\right)\right) \cdots \left(1 + \varepsilon_\beta \cdot \left(\frac{m}{q_\beta}\right)\right)$$

gesetzt wird, und da $\frac{1}{t(b)}$ das Maass dieser Darstellung bedeutet, so geben sämmtliche Glieder, für welche die Formen $\beta(y_\varrho)$ den gleichen Werth m haben, zusammengenommen $\frac{\varpi(m)}{m^{2+2\varrho}}$ mal dem Maasse aller eigentlichen Darstellungen von m durch die Reciproken derjenigen Formen, welche das Geschlecht G' repräsentiren. Wird also dieses Maass $\mathfrak{M}(m)$ genannt, so geht die Summe (33) in die einfache Gestalt über:

$$S = \lim_{\varrho = 0} \varrho \sum_m \frac{\varpi(m) \cdot \mathfrak{M}(m)}{m^{2+2\varrho}}. \tag{36}$$

Zur Ermittelung von $\mathfrak{M}(m)$ muss dem Geschlechte G' quaternärer das Geschlecht $\Gamma'_{(\mathrm{I})}$ ternärer Formen

$$c(z_\varrho) = \sum_1^3 c_{i\varkappa} z_i z_\varkappa$$

an die Seite gestellt werden, dessen Ordnung

$$\begin{pmatrix} 1, & m \\ 1, & 1 \end{pmatrix} \tag{37}$$

und dessen Charaktere, wenn c_k analog definirt wird, wie b_k, die Werthe der Symbole

$$\left(\frac{c_2}{p_i}\right) = \left(\frac{-b}{p_i}\right) \tag{38}$$

für die μ verschiedenen Primfaktoren $p_1, p_2, \cdots p_\mu$ von m sind; c_2 darf hierbei durch irgend eine zu p_i prime Zahl $\varkappa$ ersetzt werden, welche durch die Reciproke von $c(z_\varrho)$ darstellbar ist, sodass

$$\left(\frac{\varkappa}{p_i}\right) = \left(\frac{-b}{p_i}\right).$$

Die Eisenstein'sche Formel für das Maass eines ternären Geschlechts liefert daher für das Maass des eben bezeichneten folgenden Ausdruck:

$$\frac{1}{12}\left(1 - \frac{1}{2}\left(\frac{b}{m}\right)\right) \cdot \frac{m}{2^\mu} \cdot \prod_{p_i} \left(1 + \left(\frac{b}{p_i}\right)\frac{1}{p_i}\right)$$

und folglich

$$\mathfrak{M}(m) = \frac{m}{12}\left(1 - \frac{1}{2}\left(\frac{b}{m}\right)\right) \cdot \prod_{p_i} \left(1 + \left(\frac{b}{p_i}\right)\frac{1}{p_i}\right).$$

Durch Einsetzen dieses Ausdrucks in (36) ergiebt sich

$$S = \lim_{\varrho=0} \varrho \sum_m \left(\frac{1}{12}\left(1 - \frac{1}{2}\left(\frac{b}{m}\right)\right) \frac{\varpi(m)}{m^{1+2\varrho}} \cdot \prod_p \left(1 + \left(\frac{b}{p}\right)\frac{1}{p}\right)\right), \tag{39}$$

die letztere Multiplikation auf alle Primfaktoren des jedesmaligen m erstreckt. Nun zerlegt sich $\varpi(m)$ durch Entwickelung seines Produktausdrucks in 2^β Summanden von der Form $\pm\left(\frac{m}{Q}\right)$, wo Q jeden Theiler des Produkts $q_1 \cdot q_2 \cdots q_\beta$ oder

jeden solchen Theiler von b bedeutet, der aus lauter verschiedenen Primfaktoren besteht. Dementsprechend zerfällt auch S in ebenso viel Summanden, deren jeder einzelne folgende Form haben wird:

$$\frac{1}{12}\lim.\ \varrho\, T_\varrho - \frac{1}{24}\lim.\ \varrho\, T_\varrho', \tag{40}$$

wenn man setzt:

$$\begin{cases} T_\varrho = \sum\limits_m \left(\dfrac{\left(\frac{m}{Q}\right)}{m^{1+2\varrho}} \cdot \prod\limits_p \left(1 + \left(\frac{b}{p}\right)\frac{1}{p}\right)\right) \\ T_\varrho' = \sum\limits_m \left(\dfrac{\left(\frac{b}{m}\right)\left(\frac{m}{Q}\right)}{m^{1+2\varrho}} \cdot \prod\limits_p \left(1 + \left(\frac{b}{p}\right)\frac{1}{p}\right)\right). \end{cases} \tag{41}$$

Zur weiteren Umformung verwende man die voraufgeschickte Hilfsformel (29), indem man in derselben unter N die Zahl $2b$ versteht. Die linke Seite dieser Formel wird dann identisch mit T_ϱ, wenn man

$$\psi(m) = \left(\frac{b}{m}\right)\frac{1}{m}, \quad \Psi(m) = \frac{\left(\frac{m}{Q}\right)}{m^{1+2\varrho}}$$

setzt, Funktionen, welche offenbar die dort vorausgesetzten Bedingungen erfüllen, und ebenso wird sie identisch mit T_ϱ', wenn man

$$\psi(m) = \left(\frac{b}{m}\right)\frac{1}{m}, \quad \Psi(m) = \frac{\left(\frac{b}{m}\right)\left(\frac{m}{Q}\right)}{m^{1+2\varrho}}$$

setzt, wovon dasselbe gilt wie vorher. Folglich kann man den Formeln (41) auch diese Gestalt geben:

$$T_\varrho = \frac{\sum\left(\frac{m}{Q}\right)\frac{1}{m^{1+2\varrho}} \cdot \sum\left(\frac{b}{m}\right)\left(\frac{m}{Q}\right)\frac{1}{m^{2+2\varrho}}}{\sum \frac{1}{m^{4(1+\varrho)}}}$$

$$T_\varrho' = \frac{\sum\left(\frac{b}{m}\right)\left(\frac{m}{Q}\right)\frac{1}{m^{1+2\varrho}} \cdot \sum\left(\frac{m}{Q}\right)\frac{1}{m^{2+2\varrho}}}{\sum \frac{1}{m^{4(1+\varrho)}}}.$$

Im letzteren Ausdrucke kann

ist aber $b \equiv 1 \pmod{4}$, so ist

$$S = \frac{\varphi(2b)}{90b} \cdot \frac{\sum \left(\frac{b}{m}\right) \frac{1}{m^2}}{S_4 \cdot \prod \left(1 - \frac{1}{q^4}\right)}.$$

Werden nunmehr diese beiden Werthe von S mit dem zuvor auf anderem Wege gefundenen Werthe (35) verglichen, so ergiebt sich das Maass des Geschlechts $\Gamma_{(\mathrm{I})}$ oder die Grösse M_{I}, nämlich

wenn $b \equiv 3 \pmod{4}$ ist,

$$\text{(42a)} \qquad M_{\mathrm{I}} = \frac{1}{2^\beta} \cdot \frac{b^{3/2}}{12\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2},$$

wenn aber $b \equiv 1 \pmod{4}$ ist,

$$\text{(42b)} \qquad M_{\mathrm{I}} = \frac{1}{2^\beta} \cdot \frac{b^{3/2}}{24\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2};$$

die hier auftretende Summation umfasst alle positive gegen $2b$ prime Zahlen*).

---

*) Auf gleichem Wege, wie das Maass M_{I} gefunden wurde, kann das Maass auch für jedes Geschlecht quaternärer Formen bestimmt werden. Man findet insbesondere für das Maass eines Geschlechts von Formen der Ordnung

$$\begin{pmatrix} o_1, & o_2, & o_3 \\ 1, & 1, & 1 \end{pmatrix}$$

mit lauter ungeraden Invarianten den nachstehenden Ausdruck:

$$M = \frac{\zeta}{12} \cdot \frac{o_1^{3/2} o_2^2 o_3^{3/2}}{2^{\iota+\varkappa+\lambda}} \cdot \prod_{q_2} \frac{1 + \left[\left(\frac{-o_1 f_2'}{q_2}\right) + \left(\frac{-o_3 f_2'}{q_2}\right)\right] \frac{1}{q_2} + \left(\frac{o_1 o_3}{q_2}\right) \frac{1}{q_2^2}}{1 - \frac{1}{q_2^2}}$$

$$\cdot \prod_{q_{12}} \left(1 + \left(\frac{-o_3 f_2'}{q_{12}}\right) \frac{1}{q_{12}}\right) \cdot \prod_{q_{23}} \left(1 + \left(\frac{-o_1 f_2'}{q_{23}}\right) \frac{1}{q_{23}}\right)$$

$$\cdot \prod_{q_{13}} \left(1 + \left(\frac{-o_2 f_1' f_3'}{q_{13}}\right) \frac{1}{q_{13}}\right) \cdot \prod_{q_{123}} \left(1 - \frac{1}{q_{123}^2}\right)$$

$$\cdot \frac{1}{\pi^2} \sum \left(\frac{\Delta}{m}\right) \frac{1}{m^2}.$$

Darin bezeichnet q_2 alle nur in der zweiten der Invarianten o_1, o_2, o_3 aufgehenden Primzahlen, q_{12} die in o_1, o_2 aber nicht in o_3 aufgehenden; analoge Bedeutung haben q_{13}, q_{23}, während q_{123} die allen drei Invarianten gemeinsamen Primzahlen bezeichnet; die Produkte sind auf

Durch eine analoge Betrachtung bestimmt man das Maass M_{II} des Geschlechts $\Gamma_{(II)}$, so oft dasselbe vorhanden ist, d. h. wenn $b \equiv 5$ (mod. 8) ist, findet sich

$$M_{II} = \frac{1}{2^{\beta}} \cdot \frac{b^{3/2}}{60\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}. \tag{43}$$

Daher ist für diesen Fall

$$M_I + M_{II} = \frac{1}{2^{\beta}} \cdot \frac{7b^{3/2}}{120\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}. \tag{44}$$

Und somit wird mit Rücksicht auf (26) nachstehender Satz gewonnen:

Die Anzahl aller eigentlichen Darstellungen als Summe von fünf Quadraten beträgt für Zahlen b von einer der beiden Formen $8\varkappa + 3, 7$

$$A_{3,7} = \frac{160 \cdot b^{3/2}}{\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}, \tag{45a}$$

für Zahlen b von der Form $8\varkappa + 1$

$$A_1 = \frac{80 \cdot b^{3/2}}{\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}, \tag{45b}$$

und für Zahlen b von der Form $8\varkappa + 5$

$$A_5 = \frac{112 \cdot b^{3/2}}{\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}. \tag{45c}$$

Eine Betrachtung ähnlich derjenigen in nr. 3 des achten Capitels lässt unschwer erkennen, dass die Darstellungen einer Zahl $b = 8\varkappa + 5$ als Summe von fünf ungeraden Quadraten und die Darstellungen der Formen $b(y_{\varrho})$ aus dem Geschlechte $\Gamma_{(II)}$ adjungirt sein müssen. Demnach muss die Anzahl der

diese einzelnen Categorieen zu erstrecken. Ferner ist ι die Anzahl aller in o_1, $\varkappa$ die Anzahl aller in o_2, λ die Anzahl aller in o_3 aufgehenden Primzahlen und ζ ist gleich

$$\frac{1}{2}(2 + \delta) = \frac{1}{2}\left(2 + (-1)^{\frac{1}{4}(o_1+1)(o_2+1) + \psi(o,3)}\right)$$

oder gleich 1, jenachdem $o_1\, o_3 \equiv 1$ oder 3 (mod. 4) ist.

Vgl. zu dieser Formel Smith' Abhandlung sur la représentation des nombres par une somme de cinq carrés (Mém. prés. par div. Sav. Etr. t. 29), in welcher das Maass eines Geschlechts quaternärer Formen auch für die hier übergangenen Fälle gerader Formen und Determinanten gegeben wird.

eigentlichen Darstellungen einer Zahl b von der Form $8\varkappa + 5$ als Summe von fünf *ungeraden* Quadraten

$$A_5' = 1920 \cdot 2^3\, \mathsf{M}_{\mathrm{II}}$$

d. i.

(45d) $$A_5' = \frac{32 b^{3/2}}{\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}$$

sein.

Hiernach wäre $A_5 - A_5' = A_1$ die Anzahl der eigentlichen Darstellungen einer Zahl b von der Form $8\varkappa + 5$ als Summe von fünf Quadraten, die nicht sämmtlich ungerade sind; bei Darstellungen von Zahlen der drei anderen Formen $8\varkappa + 1, 3, 7$ sind die fünf Quadrate niemals sämmtlich ungerade. Demnach kann man auch folgenden Satz aufstellen, indem man die verschiedenen Formeln in eine einzige zusammenzieht: Ist b irgend eine positive ungerade Zahl, so ist die Anzahl ihrer Darstellungen als Summe von fünf nicht sämmtlich ungeraden Quadraten gleich

(46) $$\frac{40}{\pi^2}\left(3 - (-1)^{\left[\frac{b}{2}\right]}\right) \cdot b^{3/2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}.$$

Letztere Formel bleibt sogar auch für gerade Zahlen in Geltung*).

8. Wir wenden uns nunmehr zur Ermittelung des Maasses für ein beliebiges Geschlecht positiver quadratischer Formen mit $n > 4$ Veränderlichen, indem wir uns dabei aber wieder auf den einfachsten Fall ungerader Formen mit einer ungeraden Determinante beschränken. Man kann zu diesem Behufe die bisher besprochenen Methoden verwenden, indem man von Formen mit $n - 1$ Veränderlichen zu solchen mit n Veränderlichen aufsteigt und dabei passend für ein ungerades n die bei den ternären, für ein gerades n die bei den quaternären Formen benutzten Wege einschlägt. Jedoch folgt man bei dieser allgemeinen Untersuchung besser derjenigen Methode, welche Minkowski zuletzt**) angegeben hat, weil dieselbe auf sehr schöne und instructive

*) S. Minkowski, mém. sur la théorie des formes quadratiques, p. 164.

**) Minkowski, Untersuchungen über quadratische Formen, Acta math. 7.

Weise die Bedeutung der einzelnen Theile lehrt, aus welchen sich der Ausdruck des Maasses zusammensetzt. Die Ueberlegung, aus welcher diese Methode entspringt, ist die folgende.

Mit $f(N)$ haben wir die Anzahl aller Substitutionen T bezeichnet, deren Modulus $\equiv 1$ (mod. N) ist und welche den Rest von $f(x_\varrho)$ (mod. N) nicht verändern. Wie wir nun die reciproke Anzahl der Substitutionen, deren Modulus gleich 1 ist und welche $f(x_\varrho)$ selbst nicht verändern, das Maass der Form $f(x_\varrho)$ oder ihrer Classe genannt haben, so liesse sich entsprechend $\frac{1}{f(N)}$ als das Maass derselben (mod. N) bezeichnen, und da diese Grösse für alle Formen desselben Geschlechts nach den für sie abgeleiteten Formeln unveränderlich ist, vermuthen, dass sie für das Maass des Geschlechts eine Bedeutung habe. Solche Vermuthung wird fester begründet durch die Bemerkung, dass die Anzahl aller Formen in der Classe von $f(x_\varrho)$ ein Vielfaches von der in nr. 6 des achten Capitels mit $\mathfrak{N}$ bezeichneten Anzahl sein muss. In der That, jede Form der Classe von $f(x_\varrho)$ lässt (mod. N) einen der $\mathfrak{N}$ Reste $g_1, g_2, \cdots g_{\mathfrak{N}}$; $f(x_\varrho)$ selbst etwa den Rest g_1; mit

$$f_1 = f(x_\varrho),\ f_1',\ f_1'',\ \cdots$$

mögen die sämmtlichen Formen der Classe von $f(x_\varrho)$ bezeichnet werden, welche $\equiv g_1$ (mod. N) sind. Ist dann S_i eine unimodulare Substitution, welche $f(x_\varrho)$ in eine mit g_i (mod. N) congruente Form f_i verwandelt, so haben die unter einander verschiedenen Formen

$$f_i,\ f_i',\ f_i'',\ \cdots$$

welche aus $f_1, f_1', f_1'', \cdots$ resp. durch die Substitution S_i hervorgehen, ebenfalls (mod. N) den Rest g_i, ausser ihnen ist aber in der Classe von $f(x_\varrho)$ keine Form weiter vorhanden, welche ihn hätte. Denn, wäre noch φ eine solche, also $\varphi \equiv g_i$ (mod. N), so würde daraus durch die Substitution S_i^{-1} eine mit g_1 (mod. N) congruente Form der Classe also eine von den Formen $f_1, f_1', f_1'', \cdots$ hervorgehen und somit φ mit einer der Formen $f_i, f_i', f_i'', \cdots$ übereinstimmen. Da sonach jedem der Reste $g_1, g_2, \cdots g_{\mathfrak{N}}$ gleichviel Formen der Classe zugehören,

ist ihre gesammte Menge ein Vielfaches von $\mathfrak{N}$, in dem Sinne, dass sie in $\mathfrak{N}$ Complexe zerfällt, deren einzelne Formen sich eindeutig entsprechend coordinirt werden können. Ist dies aber der Fall, so zeigt der im achten Capitel gegebene Ausdruck (32) für die Anzahl $\mathfrak{N}$, dass die Anzahl der Formen in jeder Classe des Geschlechts in dem eben bezeichneten Sinne, welches auch N sei, den Faktor $\frac{1}{f(N)}$ und folglich zugleich mit den Faktoren $\frac{1}{f(2^{\mathfrak{f}})}, \frac{1}{f(p^{\mathfrak{f}})}$ die sämmtlichen Faktoren

$$(47) \qquad \frac{1}{f[2]}, \frac{1}{f[3]}, \frac{1}{f[5]}, \cdots \frac{1}{f[p]}, \cdots$$

haben wird, unter p jede ungerade Primzahl verstanden. Da ferner das Maass $\frac{1}{t(f)}$ der Classe von $f(x_\varrho)$ das Verhältniss zwischen der unendlichen Anzahl der Formen in der Classe und der gleichfalls unendlich grossen Anzahl aller unimodularen Substitutionen ist, so wird sich jener Umstand auf das Maass des Geschlechts übertragen und somit die Grössen (47) als wesentliche Faktoren des Ausdrucks dieses Maasses erwartet werden dürfen.

Dies ist nun in der That zutreffend, denn der Ausdruck für das Maass M eines Geschlechts lautet allgemein folgendermassen:

$$(48) \qquad M = c_n \cdot \frac{\sqrt{\Omega}}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \prod_q \frac{1}{f[q]};$$

die hierin auftretende Multiplikation erstreckt sich auf sämmtliche Primzahlen $2, 3, 5, 7, 11, \cdots$ in natürlicher Reihenfolge und es ist zu setzen:

$$\Omega = \prod_{h=1}^{n-1} o_h^{h(n-h)}$$

$$c_n = 2 \cdot \frac{\Gamma\left(\frac{1}{2}\right) \Gamma\left(\frac{2}{2}\right) \cdots \Gamma\left(\frac{n}{2}\right)}{\Gamma\left(\frac{1}{2}\right)^{\frac{n(n+1)}{2}}} \text{*)}.$$

*) S. die letztangeführte Arbeit von Minkowski, wo dieser Ausdruck ohne Einschränkung für jedes Geschlecht von Formen mit n Veränderlichen bewiesen wird

Vor allem soll gezeigt werden, dass dieser Ausdruck einen endlichen Werth darstellt. Hierzu bemerke man die bekannte Gleichung

$$\prod_q \frac{1}{1-\frac{1}{q^{2\varkappa}}} = \sum_{s=1}^{\infty} \frac{1}{s^{2\varkappa}},$$

in welcher die Multiplikation zur Linken den gleichen Umfang hat wie in (48). Schreibt man kurz $S_{2\varkappa}$ statt der Summe zur Rechten, so geht die Gleichheit

$$1 = S_{2\varkappa} \cdot \prod_q \left(1-\frac{1}{q^{2\varkappa}}\right)$$

und daraus die allgemeinere:

$$1 = S_2 \cdot S_4 \cdots S_{2\cdot\left[\frac{n-1}{2}\right]}$$
$$\cdot \prod_q \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)$$

hervor. Indem wir diese mit der Gleichung (48) multipliciren und zur Abkürzung

$$(49) \qquad \frac{\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)}{f[q]} = E(q)$$

setzen, bringen wir jene Gleichung in folgende Gestalt:

$$(50) \quad M = c_n \cdot \frac{\sqrt{\Omega}}{\sigma_1\,\sigma_2 \cdots \sigma_{n-1}} \cdot S_2 \cdot S_4 \cdots S_{2\left[\frac{n-1}{2}\right]} \cdot \prod_q E(q).$$

Nun zerfallen die sämmtlichen Primzahlen q in drei Categorieen: die Primzahl 2, die in Δ aufgehenden, welche $\mathfrak{d}$ heissen mögen und deren Anzahl nur eine endliche ist, und die unendlich vielen nicht in 2Δ aufgehenden Primzahlen, die mit p bezeichnet werden sollen. Für jede solche Primzahl p ist in der Formel (49) des achten Capitels $\lambda = 1$ zu setzen und man findet nach (44) und (47) daselbst

wenn n ungerade ist,

$$E(p) = 1,$$

ist ihre gesammte Menge ein Vielfaches vo dass sie in $\mathfrak{N}$ Complexe zerfällt, deren eindeutig entsprechend coordinirt w aber der Fall, so zeigt der im ac druck (32) für die Anzahl $\mathfrak{N}$, d jeder Classe des Geschlechts i Hiernach welches auch N sei, den F mit den Faktoren $\frac{1}{f(2^{\lambda})}$,

(47) $\frac{1}{f[2}$ ... $= \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}}$,

haben wird, unte

ferner das M ... $\frac{\Delta}{p}\Bigr) \frac{1}{p^{\frac{n}{2}}}$.

zwischen de

der gleich ...ation auf alle positive gegen 2Δ prime ganze stitutio ...rstreckt wird. Ferner ist bekanntlich Gesch lich d

$$S_{2\varkappa} = \frac{1}{2} B_\varkappa \cdot \frac{(2\pi)^{2\varkappa}}{1 \cdot 2 \cdot 3 \cdots 2\varkappa},$$

$B_\varkappa$ die $\varkappa^{\text{te}}$ Bernoulli'sche Zahl bedeutet, sodass

$$B_1 = \frac{1}{6},\ B_2 = \frac{1}{30},\ B_3 = \frac{1}{42}, \cdots$$

ist. Führt man diese Werthe in die Formel (50) ein, so geht sie nach den einfachsten Eigenschaften der Γ-Funktionen in folgende Gestalt über:

wenn n gerade ist:

$$\text{(51a)} \quad \begin{cases} M = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot \dfrac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{\pi^{\frac{n}{2}}} \cdot \dfrac{\sqrt{\Omega} \cdot E(2)}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \\ \qquad \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}) \cdot \sum \left(\dfrac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \dfrac{1}{m^{\frac{n}{2}}}; \end{cases}$$

wenn n ungerade ist:

$$\text{(51b)} \quad M = \left(\frac{1}{2}\right)^{\frac{n-3}{2}} \cdot \frac{B_1 B_2 \cdots B_{\frac{n-1}{2}}}{1 \cdot 2 \cdots \frac{n-1}{2}} \cdot \frac{\sqrt{\Omega} \cdot E(2)}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}),$$

…ke, welche, nur aus einer endlichen Anzahl von Fak-
…ehend, selbst endliche Werthe darstellen. Für den
der Formen mit ungerader Determinante ist das
$\cdots \sigma_{n-1}$ durch Eins zu ersetzen.
t aber diese Ausdrücke auch als die für das
…hts giltigen zu erweisen, bestätigen wir sie
ll ternärer Formen. Der betreffende Aus-
Falle folgendermassen:

$$\ldots o_2 \cdot E(2) \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}),$$

in $\Delta = o_1^2 o_2$ aufgehenden Primfak-
Diese unterscheide man nun in die Prim-
welche nur in o_1, in die Primfaktoren q_2, welche
o_2, und in die Primfaktoren q_{12}, welche gemeinsam in
o_1, o_2 aufgehen. Dann kann man zunächst schreiben:

$$M = B_1 \cdot o_1 o_2 \cdot E(2) \cdot \prod E(q_1) \cdot \prod E(q_2) \cdot \prod E(q_{12}),$$

während allgemein

$$E(q) = \frac{1 - \frac{1}{q^2}}{f[q]}$$

ist. Wenn nun

1) $q = q_1$ ist, so hat man für einen Hauptrepräsentanten des Geschlechts (mod. $q_1{}^t$) die Congruenz

$$f' \equiv \alpha x^2 + q_1^{\omega_1}(\alpha' x'^2 + \alpha'' x''^2).$$

Man hat also, um die Formeln der nr. 8, 9 des achten Capitels anzuwenden, $\lambda = 2$, $f[q_1] = 2\mathfrak{P}_1\mathfrak{P}_2$ zu setzen, und da

$$\mathfrak{P}_1 = 1,\ \mathfrak{P}_2 = 1 - \left(\frac{-\alpha'\alpha''}{q_1}\right)\frac{1}{q_1},$$

endlich, wenn $o_1 = q^{\omega_1} \cdot e_1$ gesetzt wird,

$$e_1^2 o_2 \equiv \alpha\alpha'\alpha'' \pmod{q_1}$$

also

$$\left(\frac{-\alpha'\alpha''}{q_1}\right) = \left(\frac{-\alpha o_2}{q_1}\right) = \left(\frac{-f_1' o_2}{q_1}\right)$$

gefunden wird, kommt

$$E(q_1) = \frac{1}{2} \cdot \frac{1 - \frac{1}{q_1^2}}{1 - \left(\frac{-f_1' o_2}{q_1}\right)\frac{1}{q_1}} = \frac{1}{2} \cdot \left(1 + \left(\frac{-f_1' o_2}{q_1}\right)\frac{1}{q_1}\right).$$

wenn n gerade ist,

$$E(p) = \frac{1}{1 - \left(\frac{(-1)^{\frac{n}{2}} \Delta}{p}\right) \frac{1}{p^{\frac{n}{2}}}},$$

da $\alpha_1 \alpha_1' \cdots \alpha_1^{(n-1)} \equiv \Delta \pmod{p}$ gefunden wird. Hiernach ist im ersteren Falle

$$\prod_p E(p) = 1,$$

im letzteren

$$\prod_p E(p) = \prod_p \frac{1}{1 - \left(\frac{(-1)^{\frac{n}{2}} \Delta}{p}\right) \frac{1}{p^{\frac{n}{2}}}} = \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}},$$

wenn die Summation auf alle positive gegen 2Δ prime ganze Zahlen m erstreckt wird. Ferner ist bekanntlich

$$S_{2\varkappa} = \frac{1}{2} B_\varkappa \cdot \frac{(2\pi)^{2\varkappa}}{1 \cdot 2 \cdot 3 \cdots 2\varkappa},$$

wo $B_\varkappa$ die $\varkappa^{\text{te}}$ Bernoulli'sche Zahl bedeutet, sodass

$$B_1 = \frac{1}{6}, \; B_2 = \frac{1}{30}, \; B_3 = \frac{1}{42}, \cdots$$

ist. Führt man diese Werthe in die Formel (50) ein, so geht sie nach den einfachsten Eigenschaften der Γ-Funktionen in folgende Gestalt über:

wenn n gerade ist:

$$(51\text{a}) \quad \begin{cases} M = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot \dfrac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{\pi^{\frac{n}{2}}} \cdot \dfrac{\sqrt{\Omega} \cdot E(2)}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \\ \qquad \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}) \cdot \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}}; \end{cases}$$

wenn n ungerade ist:

$$(51\text{b}) \quad M = \left(\frac{1}{2}\right)^{\frac{n-3}{2}} \cdot \frac{B_1 B_2 \cdots B_{\frac{n-1}{2}}}{1 \cdot 2 \cdots \frac{n-1}{2}} \cdot \frac{\sqrt{\Omega} \cdot E(2)}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}),$$

Ausdrücke, welche, nur aus einer endlichen Anzahl von Faktoren bestehend, selbst endliche Werthe darstellen. Für den Fall ungerader Formen mit ungerader Determinante ist das Produkt $\sigma_1 \sigma_2 \cdots \sigma_{\varkappa-1}$ durch Eins zu ersetzen.

9. Um jetzt aber diese Ausdrücke auch als die für das Maass des Geschlechts giltigen zu erweisen, bestätigen wir sie vor allem für den Fall ternärer Formen. Der betreffende Ausdruck lautet in diesem Falle folgendermassen:

$$M = B_1 \cdot o_1 o_2 \cdot E(2) \cdot \prod_{\mathfrak{d}} E(\mathfrak{d}),$$

wo $\mathfrak{d}$ die verschiedenen in $\Delta = o_1^2 o_2$ aufgehenden Primfaktoren bezeichnet. Diese unterscheide man nun in die Primfaktoren q_1, welche nur in o_1, in die Primfaktoren q_2, welche nur in o_2, und in die Primfaktoren q_{12}, welche gemeinsam in o_1, o_2 aufgehen. Dann kann man zunächst schreiben:

$$M = B_1 \cdot o_1 o_2 \cdot E(2) \cdot \prod E(q_1) \cdot \prod E(q_2) \cdot \prod E(q_{12}),$$

während allgemein

$$E(q) = \frac{1 - \frac{1}{q^2}}{f[q]}$$

ist. Wenn nun

1) $q = q_1$ ist, so hat man für einen Hauptrepräsentanten des Geschlechts (mod. q_1^t) die Congruenz

$$f' \equiv \alpha x^2 + q_1^{\omega_1}(\alpha' x'^2 + \alpha'' x''^2).$$

Man hat also, um die Formeln der nr. 8, 9 des achten Capitels anzuwenden, $\lambda = 2$, $f[q_1] = 2 \mathfrak{P}_1 \mathfrak{P}_2$ zu setzen, und da

$$\mathfrak{P}_1 = 1,\ \mathfrak{P}_2 = 1 - \left(\frac{-\alpha'\alpha''}{q_1}\right)\frac{1}{q_1},$$

endlich, wenn $o_1 = q^{\omega_1} \cdot e_1$ gesetzt wird,

$$e_1^2 o_2 \equiv \alpha \alpha' \alpha'' \pmod{q_1}$$

also

$$\left(\frac{-\alpha'\alpha''}{q_1}\right) = \left(\frac{-\alpha o_2}{q_1}\right) = \left(\frac{-f_1' o_2}{q_1}\right)$$

gefunden wird, kommt

$$E(q_1) = \frac{1}{2} \cdot \frac{1 - \frac{1}{q_1^2}}{1 - \left(\frac{-f_1' o_2}{q_1}\right)\frac{1}{q_1}} = \frac{1}{2} \cdot \left(1 + \left(\frac{-f_1' o_2}{q_1}\right)\frac{1}{q_1}\right).$$

2) Ist $q = q_2$, so erfüllt ein Hauptrepräsentant des Geschlechts (mod. $q_2{}^t$) die Congruenz

$$f' \equiv \alpha x^2 + \alpha' x'^2 + q_2{}^{\omega_2} \alpha'' x''^2,$$

also ist

$$\lambda = 2,\ f[q_2] = 2\mathfrak{P}_1 \mathfrak{P}_2 = 2\left(1 - \left(\frac{-\alpha\alpha'}{q_2}\right)\frac{1}{q_2}\right),$$

folglich wird, da $\alpha\alpha' \equiv f_2' o_1$ (mod. q_2) ist,

$$E(q_2) = \frac{1}{2}\left(1 + \left(\frac{-f_2' o_1}{q_2}\right)\frac{1}{q_2}\right).$$

3) Ist $q = q_{12}$, so besteht für einen Hauptrepräsentanten des Geschlechts (mod. q_{12}^t) die Congruenz

$$f' \equiv \alpha x^2 + \alpha' q_{12}^{\omega_1} x'^2 + q_{12}^{\omega_1 + \omega_2} \cdot \alpha'' x''^2$$

also ist

$$\lambda = 3,\ f[q_{12}] = 4\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3 = 4$$

und somit

$$E(q_{12}) = \frac{1}{4}\left(1 - \frac{1}{q_{12}^2}\right).$$

4) Ist endlich $q = 2$, so ist, da $n = 3$ ungerade ist,

$$f[2] = 2\left(1 - \frac{1}{2^2}\right) \cdot \left(1 + \frac{\delta}{2}\right)^{-1},$$

somit

$$E(2) = \frac{1}{2}\left(1 + \frac{\delta}{2}\right) = \frac{2 + \delta}{4},$$

wo man nun mit Rücksicht auf den Ausdruck der Einheit δ sowie auf die Möglichkeitsbedingung (86) des sechsten Capitels ohne Mühe die Uebereinstimmung von δ mit der in der ersten Abtheilung mit E bezeichneten Einheit feststellt und dann für M folgende Gleichung findet:

$$M = \frac{1}{24} o_1 o_2 \cdot \frac{2 + E}{2^{\varkappa + \lambda}} \cdot \prod\left(1 + \left(\frac{-f_1' o_2}{q_1}\right)\frac{1}{q_1}\right)$$
$$\cdot \prod\left(1 + \left(\frac{-f_2' o_1}{q_2}\right)\frac{1}{q_2}\right) \cdot \prod\left(1 - \frac{1}{q_{12}^2}\right),$$

worin $\varkappa$, λ die Anzahl der Primfaktoren bedeuten, aus denen resp. o_1 und o_2 bestehen, eine Gleichung, die bis auf verschiedene Bezeichnung der entsprechenden Grössen mit der in der ersten Abtheilung gefundenen Eisenstein'schen Formel (S. 191) vollkommen identisch ist.

Verfährt man in gleicher Weise, so überzeugt man sich

auch für quaternäre Formen der bezeichneten Art von der Uebereinstimmung der in der Anmerkung gegebenen Formel für das Maass derselben mit der aus (51a) für $n = 4$ sich ergebenden Gleichung

$$M = \frac{B_1}{\pi^2} \cdot o_1^{3/2} o_2^{2} o_3^{3/2} \cdot E(2) \cdot \prod E(\mathfrak{d}) \cdot \sum \left(\frac{\Delta}{m}\right) \frac{1}{m^2}.$$

Zum allgemeinen Beweise der Formeln (51a) und (51b) bedienen wir uns des Schlusses von $n - 1$ auf n: wir setzen voraus, ihre Richtigkeit sei bereits erwiesen für die Geschlechter ungerader Formen mit ungerader Determinante und mit $n - 1$ Veränderlichen, und zeigen, dass sie dann auch gelten für solche Formen mit n Veränderlichen; da sie für ternäre (und quaternäre) Formen der bezeichneten Art erwiesen sind, gelten sie dann allgemein. Die zu diesem Zwecke anzustellende Untersuchung beruht nun wieder auf den Dirichlet'schen Methoden und nimmt einen ganz ähnlichen Gang, wie in den bereits erörterten speciellen Fällen.

Sei ein bestimmtes Geschlecht G von positiven Formen der bezeichneten Art mit n Veränderlichen gegeben, indem sowohl die Ordnung

$$\begin{matrix} o_1, & o_2, & \cdots & o_{n-1} \\ 1, & 1, & \cdots & 1 \end{matrix}$$

als auch die Charaktere desselben, letztere so, dass die Möglichkeitsbedingung erfüllt wird, bestimmt gegeben werden. Sei Δ die Determinante der Formen dieses Geschlechts und R eine später zu bestimmende gegen 2Δ prime ganze Zahl. Unter den Formen des Geschlechts lässt sich dann eine (mod. $8\Delta R$) charakteristische Form φ aussuchen, ihr erster Coefficient, der prim ist gegen $8\Delta R$, heisse α. Sind ∂ die ungeraden Primfaktoren von Δ und $\mathfrak{d}$ ihre Anzahl, sind ebenso r die ungeraden Primfaktoren von R und $\mathfrak{r}$ ihre Anzahl, so wird die Zahl α in Bezug auf jeden von ihnen sowohl, als mit Bezug auf die Moduln 4 und 8 bestimmte quadratische Charaktere haben:

$$(52) \qquad (-1)^{\frac{\alpha-1}{2}}, \ \left(\frac{2}{\alpha}\right), \ \left(\frac{\alpha}{\partial}\right), \ \left(\frac{\alpha}{r}\right).$$

Da nun die Classen eines Geschlechts nach jedem Modulus,

wenn ihre Formen in passender Reihenfolge gedacht werden, die gleichen Reste lassen, so kann man aus jeder derselben eine Form auswählen, welche (mod. $8\Delta R$) congruent ist mit φ. Die so gewählten Repräsentanten seien

$$f_1, f_2, f_3, \cdots, \tag{53}$$

f irgend einer von ihnen. Man betrachte alsdann folgende Summe:

$$S = \varrho \sum \frac{1}{f(\xi_i)^{\frac{n}{2}(1+\varrho)}}, \tag{54}$$

indem man sie über alle Werthsysteme $\xi_1, \xi_2, \cdots \xi_n$ erstreckt, für welche, wenn

$$f(\xi_i) = m$$

gesetzt wird, die Zahl m prim gegen $8\Delta R$ und von gleichen quadratischen Charakteren mit Bezug auf 4 und 8 und die Primfaktoren von ΔR ist, wie α; doch darf nicht

$$\xi_1 \equiv \xi_2 \equiv \cdots \equiv \xi_n \equiv 1 \pmod{2} \tag{55}$$

sein.

Der Vorschrift zufolge ist m von derselben Linearform $8x + 1, 3, 5, 7$ wie α und nach jedem Primfaktor p von ΔR einem unter $\frac{p-1}{2}$ bestimmten Resten (mod. p) congruent, und folglich gestatten die Zahlen m

$$\prod_p \left(\frac{p-1}{2}\right) p^{\delta-1}$$

bestimmte Reste μ (mod. $8\Delta R$), wenn p^δ die höchste in ΔR aufgehende Potenz von p ist, und die sämmtlichen gedachten Werthsysteme ξ_i sind die sämmtlichen Lösungen der Congruenzen

$$f(\xi_i) \equiv \mu \pmod{8\Delta R}, \tag{56}$$

welche die Congruenzen (55) nicht erfüllen. Nun stimmt nach den Auseinandersetzungen des siebenten Capitels die Anzahl der incongruenten dieser Lösungen für jedes der bezeichneten μ mit der der gleichartigen Lösungen der Congruenz

$$f(\xi_i) \equiv \alpha \pmod{8\Delta R} \tag{57}$$

überein, welch letztere dem Produkte der Mengen der ebenso

gearteten Lösungen der Congruenzen

$$f(\xi_i) \equiv \alpha \pmod{8}, \quad f(\xi_i) \equiv \alpha \pmod{p^{\bar\omega}}, \cdots$$

gleich ist. Den Formeln jenes Capitels entsprechend findet man die Anzahl der Lösungen der ersten dieser Congruenzen gleich $2^{3(n-1)} \cdot A_2$, wo

für ein gerades n:

$$A_2 = 1 + (\varepsilon - 1)\frac{(-1)^{\frac{\alpha-1}{2}}\delta}{2^{\frac{n}{2}-1}}, \tag{58a}$$

für ein ungerades n:

$$A_2 = \left(1 - \frac{\delta}{2^{\frac{n-1}{2}}}\right)\left(1 + \left[1 + \varepsilon\cdot(-1)^{\frac{\alpha-1}{2}}\right]\frac{\delta}{2^{\frac{n-1}{2}}}\right) \tag{58b}$$

ist. In gleicher Weise findet man für die Anzahl der (mod. $p^{\bar\omega}$) incongruenten Lösungen ξ_i dieser Art für die zweite jener Congruenzen $p^{\bar\omega(n-1)} \cdot A_p$, wenn $p^{n-1} A_p$ die Anzahl solcher Lösungen für die Congruenz

$$f(\xi_i) \equiv \alpha \pmod{p} \tag{59}$$

bezeichnet. Hiernach wird die Anzahl der (mod. $8\Delta R$) incongruenten Werthsysteme ξ_i, welche die Congruenz (57) oder (56) aber nicht die Congruenzen (55) erfüllen,

$$(8\Delta R)^{n-1} \cdot \prod A_q$$

sein, wenn sich die Multiplikation auf jede in $8\Delta R$ enthaltene Primzahl bezieht. Dies gilt für jeden der Reste μ; da aber offenbar, wenn μ', μ'' zwei verschiedene Reste (mod. $8\Delta R$) bezeichnen, auch die Werthsysteme ξ_i, welche den zugehörigen Congruenzen

$$f(\xi_i) \equiv \mu', \; f(\xi_i) \equiv \mu'' \pmod{8\Delta R}$$

genügen, verschieden sein müssen, so repräsentiren die sämmtlichen bei der Summe (54) in Betracht kommenden Werthsysteme ξ_i (mod. $8\Delta R$) genau

$$\mathsf{A} = \prod \frac{p-1}{2} p^{\bar\omega-1} \cdot (8\Delta R)^{n-1} \cdot \prod A_q$$

d. i. einfacher

$$\mathsf{A} = \frac{1}{2} \cdot (8\Delta R)^n \cdot \prod \left(\frac{1}{2}\left(1 - \frac{1}{q}\right) A_q\right). \tag{60}$$

verschiedene Restsysteme oder sie sind in einer ebenso grossen Anzahl A von Systemen arithmetischer Progressionen

$$(61)\qquad \mathfrak{x}_1 = 8\Delta R \cdot X_1 + v_1,$$
$$\mathfrak{x}_2 = 8\Delta R \cdot X_2 + v_2, \cdots \mathfrak{x}_n = 8\Delta R \cdot X_n + v_n$$

enthalten, welche sie offenbar auch erfüllen.

Zur Abkürzung sei eine frühere sehr bequeme Bezeichnung hier wieder eingeführt. Bezeichnet q sämmtliche Primzahlen, aus denen eine Zahl N zusammengesetzt ist, so heisse $(N)_n$ das Produkt

$$(62)\qquad (N)_n = \prod\left(1 - \frac{1}{q^n}\right),$$

auf alle jene Primzahlen q erstreckt.

10. Man fasse nun in der absolut convergenten und daher von der Anordnung der Glieder unabhängigen Summe S diejenigen Glieder zusammen, bei welchen die $\mathfrak{x}_i$ je einem der A Systeme arithmetischer Progressionen angehörig sind, betrachte mithin zunächst nur die über sämmtliche Werthsysteme $\mathfrak{x}_i$ von der Form (61) erstreckte Summe

$$(63)\qquad S_0 = \varrho \cdot \sum \frac{1}{f(\mathfrak{x}_i)^{\frac{n}{2}(1+\varrho)}},$$

indem man unter $v_1, v_2, \cdots v_n$ feste, unter $X_1, X_2, \cdots X_n$ aber sämmtliche positive und negative ganze Zahlen versteht. Denkt man diese Summe nach den wachsenden Werthen des Nenners geordnet, bezeichnet mit t eine beliebig wachsende positive Grösse und mit T die Anzahl derjenigen Glieder der Summe, bei welchen

$$f(\mathfrak{x}_i)^{\frac{n}{2}} \overline{\gtrless} t$$

ist, so ist nach dem fundamentalen Dirichlet'schen Satze*)

$$(64)\qquad \lim_{\varrho=0} S_0 = \lim_{t=\infty} \frac{T}{t},$$

falls der letztere Grenzwerth existirt. Das Zeichen T bedeutet aber auch die Anzahl der Werthsysteme $\mathfrak{x}_i$ von der Form (61), welche, wenn

*) S. analyt. Zahlenth. S. 68.

$$f(\xi_i) = \sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta}\, \xi_\alpha\, \xi_\beta \tag{65}$$

gesetzt wird, der Ungleichheit

$$\sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta} \cdot \frac{\xi_\alpha}{t^{\frac{1}{n}}} \cdot \frac{\xi_\beta}{t^{\frac{1}{n}}} \overline{\gtrless} 1$$

genügen; setzt man daher

$$\eta_\alpha = \frac{\xi_\alpha}{t^{\frac{1}{n}}} = \frac{8 \Delta R}{t^{\frac{1}{n}}} \cdot X_\alpha + \frac{v_\alpha}{t^{\frac{1}{n}}}, \tag{66}$$

so bedeutet T die Anzahl der „Netzpunkte“ η_α, welche der Ungleichheit

$$\sum_{(\alpha, \beta = 1, 2, \cdots n)} a_{\alpha\beta}\, \eta_\alpha\, \eta_\beta \overline{\gtrless} 1 \tag{67}$$

genügen, und somit wird, einem anderen Dirichlet'schen Satze*) zufolge

$$\lim_{t=\infty} . T \left(\frac{8 \Delta R}{t^{\frac{1}{n}}} \right)^n = \int d\eta_1 \cdot d\eta_2 \cdots d\eta_n$$

d. i.

$$\lim_{t=\infty} . \frac{T}{t} = \frac{1}{(8 \Delta R)^n} \cdot \int d\eta_1 \cdot d\eta_2 \cdots d\eta_n$$

sein, wenn die Integration über alle $\eta_1, \eta_2, \cdots \eta_n$ erstreckt wird, welche die Ungleichheit (67) erfüllen. Nach bekannter Formel**) hat das n-fache Integral und folglich auch lim. $\frac{T}{t}$ einen endlichen Werth, durch dessen Vergleichung mit (64)

$$\lim_{\varrho=0} . S_0 = \frac{1}{(8 \Delta R)^n} \cdot \frac{1}{\sqrt{\Delta}} \cdot \frac{2^{\left[\frac{n+1}{2}\right]} \pi^{\left[\frac{n}{2}\right]}}{n(n-2)(n-4) \cdots \left(n - 2\left[\frac{n-1}{2}\right]\right)} \tag{68}$$

und folglich allgemeiner mit Rücksicht auf (60)

$$\lim_{\varrho=0} . S = e_n \cdot \frac{(8 \Delta R)_1}{2^{\mathfrak{g}+\mathfrak{d}+\mathfrak{r}}} \cdot \frac{1}{\sqrt{\Delta}} \cdot \prod A_q \tag{69}$$

---

*) S. analyt. Zahlenth. S. 438 Formel (74).

**) S. ebendas. S. 446 Formel (92).

gefunden wird, wo zur Abkürzung

$$(70)\qquad \frac{2^{\left[\frac{n+1}{2}\right]}\pi^{\left[\frac{n}{2}\right]}}{n(n-2)(n-4)\cdots\left(n-2\left[\frac{n-1}{2}\right]\right)}=e_n$$

gesetzt worden ist.

Vergleichen wir jetzt mit der Summe S die Summe

$$(71)\qquad S'=\varrho\cdot\sum\frac{1}{f(\xi_i')^{\frac{n}{2}(1+\varrho)}},$$

in welcher die Werthsysteme ξ_i' diejenigen in S auftretenden Werthsysteme ξ_i bezeichnen, welche keinen gemeinsamen Theiler haben. Ist ξ_i' ein solches Werthsystem, also nicht

$$(72)\qquad \xi_1'\equiv\xi_2'\equiv\cdots\equiv\xi_n'\equiv 1 \pmod{2},$$

und ist

$$f(\xi_i')=m',$$

also m' prim zu $8\Delta R$ und von gleichen quadratischen Charakteren wie α, ist ferner d irgend eine zu $8\Delta R$ prime Zahl und $\xi_i=d\xi_i'$, so wird in

$$f(\xi_i)=m'd^2=m$$

die Zahl m prim gegen $8\Delta R$ sein und ebenfalls gleiche quadratische Charaktere haben wie α, und es kann nicht

$$(73)\qquad \xi_1\equiv\xi_2\equiv\cdots\equiv\xi_n\equiv 1 \pmod{2}$$

sein, mithin ist $\xi_1, \xi_2, \cdots \xi_n$ eins der in S auftretenden Werthsysteme. Ist umgekehrt

$$\xi_1=d\xi_1',\ \xi_2=d\xi_2',\ \cdots\ \xi_n=d\xi_n'$$

ein solches in S auftretendes Werthsystem, welches den grössten gemeinsamen Theiler d hat, so muss der letztere prim gegen $8\Delta R$ sein, da m es sein soll, die Zahlen ξ_i' sind alsdann ohne gemeinsamen Theiler und

$$f(\xi_i')=m',\quad \text{wo } m'=\frac{m}{d^2}$$

also von gleichen quadratischen Charakteren ist wie α, und da die Congruenzen (73) nicht stattfinden, können es auch nicht die Congruenzen (72), mithin ist $\xi_1', \xi_2', \cdots \xi_n'$ eins der Werthsysteme, auf welche sich die Summe S' bezieht. Hieraus ergiebt sich offenbar, dass sämmtliche bei S in Frage kommen-

den Systeme ξ_i aus sämmtlichen bei S' auftretenden Systemen ξ_i' gefunden werden, wenn man letztere mit sämmtlichen gegen $8\Delta R$ primen Zahlen d multiplicirt. Und somit gewinnt man die Beziehung

$$S = S' \cdot \sum_d \frac{1}{d^{n(1+\varrho)}}$$

folglich

$$\lim_{\varrho=0} S = \lim_{\varrho=0} S' \cdot \sum_d \frac{1}{d^n}$$

oder, da diese Summe auf alle zu $8\Delta R$ primen Zahlen zu erstrecken und

$$\sum_{s=1}^{\infty} \frac{1}{s^n} = \sum_d \frac{1}{d^n} \cdot \prod \frac{1}{1 - \frac{1}{q^n}}$$

ist,

$$(74) \qquad \lim_{\varrho=0} S = \lim_{\varrho=0} S' \cdot S_n (8\Delta R)_n .$$

Nach (69) geht hieraus die Gleichung hervor:

$$(75) \qquad \lim_{\varrho=0} S' = \frac{e_n}{S_n} \cdot \frac{(8\Delta R)_1}{(8\Delta R)_n} \cdot \frac{1}{2^{2+\mathfrak{b}+\mathfrak{r}}\sqrt{\Delta}} \cdot \prod A_q \text{*)}.$$

*) Der Grenzwerth (34) kann ganz ähnlich wie derjenige von S' direkt gefunden werden, er ergiebt sich aber auch aus der Formel (75), wenn man darin $n = 4$, $R = 1$, $\Delta = b^3$ also $\mathfrak{b} = \beta$ setzt und die Form $f(\xi_i')$ mit der Form $\beta(y_\varrho)$ identificirt. Man bemerke, dass die Charaktere $\left(\frac{\alpha}{r}\right)$ alsdann ausfallen, die Charaktere $\left(\frac{\alpha}{\mathfrak{b}}\right)$ aber nur das Geschlecht der Form $\beta(y_\varrho)$ feststellen also jeder durch sie dargestellten Zahl zukommen; dass andererseits offenbar, um L zu erhalten, die Summe S' für jede der vier Combinationen zu bilden ist, welche die Symbole $(-1)^{\frac{\alpha-1}{2}}$, $\left(\frac{2}{\alpha}\right)$ gestatten. Für jede von ihnen findet man

$$\lim. S' = \frac{e_4}{S_4} \cdot \frac{(8b)_1}{(8b)_4} \cdot \frac{1}{4 \cdot 2^{\beta} b^{3/2}} \cdot \prod A_q,$$

wo q die Primfaktoren von $2b$ zu durchlaufen hat. Da aber jeder ungerade Primfaktor q nur in der ersten Invariante von $\beta(y_\varrho)$ aufgeht, findet man nach den Formeln nr. 1 und 2 des siebenten Capitels das entsprechende $A_q = 2$. Dagegen ist

$$A_2 = 1 + (\varepsilon - 1) \frac{(-1)^{\frac{\alpha-1}{2}} \delta}{2}$$

$$\mathfrak{D}_1 = 1,\ \mathfrak{D}_2 = \left(1 - \frac{1}{q_2^{\,2}}\right)\left(1 - \frac{1}{q_2^{\,4}}\right)\cdots$$

$$\cdots\left(1 - \frac{1}{q_2^{\,n-4}}\right)\cdot\left(1 - \left(\frac{(-1)^{\frac{n}{2}}\varDelta R^2}{q_2}\right)\frac{1}{q_2^{\frac{n-2}{2}}}\right)$$

zu setzen und somit

$$E'(q_2) = \frac{1}{2}\left(1 + \left(\frac{(-1)^{\frac{n}{2}}\varDelta R^2}{q_2}\right)\frac{1}{q_2^{\frac{n-2}{2}}}\right);$$

dagegen ist für ein ungerades n

$$\mathfrak{D}_1 = 1,\ \mathfrak{D}_2 = \left(1 - \frac{1}{q_2^{\,2}}\right)\left(1 - \frac{1}{q_2^{\,4}}\right)\cdots\left(1 - \frac{1}{q_2^{\,n-3}}\right)$$

also

$$E'(q_2) = \frac{1}{2}\cdot$$

Je nach diesen beiden Fällen wird daher

$$\prod E'(q_2) = \frac{1}{2^\mu}\cdot\prod\left(1 + \left(\frac{(-1)^{\frac{n}{2}}\varDelta R^2}{q_2}\right)\frac{1}{q_2^{\frac{n-2}{2}}}\right)$$

oder

$$\prod E'(q_2) = \frac{1}{2^\mu}\cdot$$

Sei endlich 3) p einer der Primfaktoren q von $8\varDelta R$. Da die Repräsentanten (55) des Geschlechts G der (mod. $8\varDelta R$) charakteristischen Form φ congruent vorausgesetzt sind, darf man sie auch als Hauptrepräsentanten nach einer beliebig hohen Potenz q^t annehmen, gleichviel also, ob $q = 2$ oder eine ungerade Primzahl ist,

$$(81)\qquad f \equiv \begin{Bmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & q^{\omega_1}\alpha' & 0 & \cdots & 0 \\ 0 & 0 & q^{\omega_1+\omega_2}\alpha'' & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & q^{\omega_1+\cdots+\omega_{n-1}}\cdot\alpha^{(n-1)} \end{Bmatrix} \pmod{q^t}$$

setzen, wo α dieselbe Zahl bedeutet, wie bisher. Daraus folgt für die Reciproke $\mathfrak{f}$ die Congruenz

$$\mathfrak{f} \equiv \begin{Bmatrix} \beta^{(n-1)} q^{\omega_1'+\cdots+\omega_{n-1}'} & 0 & 0 \cdots 0 & 0 \\ 0 & \beta^{(n-2)} q^{\omega_1'+\cdots+\omega_{n-2}'} & 0 \cdots 0 & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot \cdots \beta' q^{\omega_1'} & 0 \\ 0 & 0 & 0 \cdots 0 & \beta \end{Bmatrix}$$

$$(\text{mod. } q^{t-\nu_{n-2}}),$$

in welcher die Zahlen $\beta, \beta', \cdots$, wie in nr. 16 des sechsten Capitels zu bestimmen sind. Setzt man nun in $\mathfrak{f}$ die erste Veränderliche gleich Null, so entsteht eine Form mit $n-1$ Veränderlichen, welche eigentlich durch sie dargestellt wird; die Determinante dieser Form findet sich ohne Schwierigkeit gleich $d_{n-2}' \cdot a_{11}$, wenn a_{11} den ersten Coefficienten von f und d_{n-2}' dasselbe für die Form $\mathfrak{f}$ bezeichnet, was d_{n-2} für die Form f; da a_{11} ohne gemeinsamen Theiler mit $8\Delta R$ also auch ohne gemeinsamen Theiler mit der doppelt genommenen Determinante von $\mathfrak{f}$ ist, muss jene Form mit $n-1$ Veränderlichen primitiv sein und ist somit ein Repräsentant $b(y_\varrho)$ des Geschlechts $\Gamma_{(\mathrm{I})}$. Nun findet man aber mit Rücksicht auf die Bestimmung der Zahlen $\beta, \beta', \cdots$ für die Reciproke der Form

$$b(y_\varrho) \equiv \begin{Bmatrix} \beta^{(n-2)} q^{\omega_1'+\cdots+\omega_{n-2}'}, & 0 \cdots\cdot & & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 \cdots & \beta' q^{\omega_1'} & 0 \\ 0 & 0 \cdots & 0 & \beta \end{Bmatrix}$$

$$(\text{mod. } q^{t-\nu_{n-2}})$$

folgende Congruenz, in welcher $t' \gtreqless t$:

$$f^{(1)}(x_\varrho) \equiv \alpha \cdot \begin{Bmatrix} \alpha' & 0 & 0 \cdots 0 \\ 0 & q^{\omega_2} \alpha'' & 0 \cdots 0 \\ \cdot & \cdot & \cdot \\ 0 & 0 & 0 \cdots q^{\omega_2+\cdots+\omega_{n-1}} \alpha^{(n-1)} \end{Bmatrix} (\text{mod. } q^{t'-\omega_1}).$$

Schreibt man demnach statt der Congruenz (81) die folgende:

$$f(x_\varrho) \equiv \alpha x^2 + q^{\omega_1} \cdot \frac{1}{\alpha} f^{(1)}(x_\varrho) \ (\text{mod. } q^{t'}),$$

so stellt $f^{(1)}(x_\varrho)$ einen Hauptrest des zu $\Gamma_{(\mathrm{I})}$ reciproken Geschlechts (mod. $q^{t'-\omega_1}$) dar.

Auf Grund der Formeln (41) und (49) resp. (55) und

(59) des achten Capitels überzeugt man sich nun, dass für alle in $8\Delta R$ aufgehenden Primzahlen q, ob sie gerade oder ungerade sind, die Gleichheit

$$f[q] = A_q \cdot f^{(1)}[q]$$

erfüllt ist, wenn A_q die in nr. 9 angegebene Bedeutung bewahrt. Daraus aber findet man,

wenn n gerade ist,

$$E'(q) = A_q \cdot E(q),$$

wenn n ungerade ist,

$$E'(q) = \frac{A_q \cdot E(q)}{1 - \frac{1}{q^{n-1}}}.$$

Dem entsprechend ist für ein gerades n

$$\prod E'(q) = \prod A_q E(q),$$

für ein ungerades n

$$\prod E'(q) = \frac{\prod A_q E(q)}{(8\Delta R)_{n-1}}.$$

Die Einsetzung der Werthe von c_{n-1} und S_{2x} und die Zusammenfassung der erhaltenen Resultate führt endlich zu dem Ergebnisse, das folgt:

Ist n gerade, so wird

$$\mathsf{M} = \frac{1}{2^\mu} \cdot \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot \frac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{1 \cdot 2 \cdots \frac{n-2}{2}} \cdot \sqrt{\Omega'} \cdot \prod A_q E(q) \cdot m^{\frac{n-2}{2}} \prod,$$

wo q dieselbe Bedeutung hat wie in der Formel (77) und $\prod$ zur Abkürzung steht für das über die Primfaktoren von m erstreckte Produkt

$$\prod \left(1 + \left(\frac{(-1)^{\frac{n}{2}} \Delta R^2}{p}\right) \frac{1}{p^{\frac{n-2}{2}}}\right),$$

folglich

$$\lim. \mathsf{S} = \frac{2}{n} \cdot \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot \frac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{1 \cdot 2 \cdots \frac{n-2}{2}} \cdot \sqrt{\Omega'} \cdot \prod A_q E(q)$$

$$\cdot \lim. \varrho \sum \left(\frac{1}{m^{1+\varrho}} \prod\right).$$

Durch Vergleichung mit der Formel (77) ergiebt sich demnach, wenn man zur Vereinfachung berücksichtigt, dass

$$e_n \cdot 1 \cdot 2 \cdot 3 \cdots \frac{n-2}{2} = \frac{2}{n} \pi^{\frac{n}{2}}$$

ist, folgender Ausdruck für M:

$$M = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot \frac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{\pi^{\frac{n}{2}}} \cdot \frac{\sqrt{\Omega} \cdot 2^{2+\mathfrak{b}+\mathfrak{r}} \cdot (8\Delta R)_n \cdot S_n}{(8\Delta R)_1} \cdot \prod E(q)$$
$$\cdot \lim. \varrho \sum \left(\frac{1}{m^{1+\varrho}} \prod\right).$$

Nun ist

$$\prod E(q) = E(2) \cdot \prod E(\partial) \cdot \prod E(r),$$

wenn wieder ∂ die Primfaktoren von Δ, r diejenigen von R durchläuft, und da R prim ist zu 2Δ, findet man

$$E(r) = \left(1 - \left(\frac{(-1)^{\frac{n}{2}} \Delta}{r}\right) \frac{1}{r^{\frac{n}{2}}}\right)^{-1}$$

also

$$\prod E(r) = \frac{\sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}}}{\sum \left(\frac{(-1)^{\frac{n}{2}} \Delta R^2}{h}\right) \frac{1}{h^{\frac{n}{2}}}},$$

wo die Summation nach m über alle zu 2Δ, die nach h über alle zu $2\Delta R^2$ prime positive Zahlen zu erstrecken ist. Hiernach ergiebt sich endlich:

$$(82) \quad \begin{cases} M = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \dfrac{B_1 B_2 \cdots B_{\frac{n-2}{2}}}{\pi^{\frac{n}{2}}} \cdot \sqrt{\Omega} \cdot E(2) \prod E(\partial) \\ \qquad \cdot \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}} \cdot M_0, \end{cases}$$

wenn

$$(83)\quad \begin{cases} \dfrac{(8\varDelta R)_1}{(8\varDelta R)_n}\cdot\dfrac{1}{2^{\mathfrak{s}+\mathfrak{d}+\mathfrak{r}}\cdot S_n}\cdot\sum\left(\dfrac{(-1)^{\frac{n}{2}}\varDelta R^2}{h}\right)\dfrac{1}{h^{\frac{n}{2}}}\cdot M_0 \\ = \lim\limits_{\varrho=0}.\ \varrho\sum\left(\dfrac{1}{m^{1+\varrho}}\prod\left(1+\left(\dfrac{(-1)^{\frac{n}{2}}\varDelta R^2}{p}\right)\dfrac{1}{p^{\frac{n-2}{2}}}\right)\right) \end{cases}$$

gesetzt wird.

Ist aber n ungerade, so wird

$$\mathsf{M}=\frac{1}{2^{\mu}}\left(\frac{1}{2}\right)^{\frac{n-5}{2}}\frac{B_1 B_2\cdots B_{\frac{n-3}{2}}}{\pi^{\frac{n-1}{2}}}\cdot\sqrt{\Omega'}\cdot\frac{\prod A_q E(q)}{(8\varDelta R)_{n-1}}\cdot m^{\frac{n-2}{2}}\sum{}';$$

q hat wieder dieselbe Bedeutung wie in der Formel (77) und zur Abkürzung steht $\sum'$ für die auf alle positive zu $8m\varDelta R^2$ prime Zahlen h bezogene Summe

$$\sum\left(\frac{(-1)^{\frac{n-1}{2}}m\varDelta R^2}{h}\right)\frac{1}{h^{\frac{n-1}{2}}}.$$

Hiernach ergiebt sich

$$\lim.\ \mathsf{S}=\frac{2}{n}\cdot\left(\frac{1}{2}\right)^{\frac{n-5}{2}}\cdot\frac{B_1 B_2\cdots B_{\frac{n-3}{2}}}{\pi^{\frac{n-1}{2}}}\cdot\sqrt{\Omega'}\cdot\frac{\prod A_q E(q)}{(8\varDelta R)_{n-1}}$$
$$\cdot\lim.\ \varrho\sum\left(\frac{1}{m^{1+\varrho}}\sum{}'\right)$$

und nun durch Vergleichung mit (77) und mit Rücksicht auf die Beziehung

$$\pi^{\frac{n-1}{2}}\cdot e_n=\frac{4}{n}\cdot 1\cdot 2\cdot 3\cdots\frac{n-1}{2}\cdot\frac{S_{n-1}}{B_{\frac{n-1}{2}}}$$

und wenn man endlich beachtet, dass in diesem Falle $E(r)=1$ ist, folgende Gleichung für M:

$$(84)\quad M=\left(\frac{1}{2}\right)^{\frac{n-3}{2}}\cdot\frac{B_1 B_2\cdots B_{\frac{n-1}{2}}}{1\cdot 2\cdots\frac{n-1}{2}}\cdot\sqrt{\Omega}\cdot E(2)\prod E(\delta)\cdot M_0,$$

wenn man

$$(85)\quad\begin{cases}\dfrac{1}{2^{2+\mathfrak{d}+\mathfrak{r}}}\cdot\dfrac{(8\Delta R)_1\cdot(8\Delta R)_{n-1}}{(8\Delta R)_n}\cdot\dfrac{S_{n-1}}{S_n}\cdot M_0\\[2ex] =\lim\limits_{\varrho=0}\varrho\sum\left(\dfrac{1}{m^{1+\varrho}}\sum\left(\dfrac{(-1)^{\frac{n-1}{2}}m\Delta R^2}{h}\right)\dfrac{1}{h^{\frac{n-1}{2}}}\right)\end{cases}$$

setzt.

12. Vergleicht man diese für gerade und ungerade n erhaltenen Formeln nun mit den behaupteten Formeln (51a) und (51b), so kommt, wie man sogleich sieht, der Nachweis für die Giltigkeit der letzteren auf den anderen hinaus, zu zeigen, dass in beiden Fällen die mit M_0 bezeichnete Grösse gleich 1 ist. Um dies noch zu leisten, wobei man sich nach dem für ternäre und quaternäre Formen schon Bewiesenen auf Werthe von $n > 4$ beschränken kann, bemerke man vor allem, dass den Formeln (82) und (84) zufolge der Werth von M_0 von der Wahl der Zahl R ganz unabhängig sein muss. Diese bisher nur insofern, als sie gegen 2Δ prim sein sollte, bestimmte Zahl R wähle man jetzt in der Weise, dass in $8\Delta R$ alle Primzahlen auftreten, welche kleiner sind als eine beliebig grosse ganze Zahl $g+1$. Die Zahlen m, welche prim sind gegen $8\Delta R$ und ihre Primfaktoren p, ebenso die Zahlen h, welche prim sind gegen $2\Delta R^2$ resp. gegen $8m\Delta R^2$, sind dann, abgesehen von der Einheit, jedenfalls grösser als g. Demnach liegt zunächst die Summe

$$\sum\left(\frac{(-1)^{\frac{n}{2}}\Delta R^2}{h}\right)\frac{1}{h^{\frac{n}{2}}}$$

zwischen den Grenzen

$$1\pm\left(\frac{1}{(g+1)^{\frac{n}{2}}}+\frac{1}{(g+2)^{\frac{n}{2}}}+\cdots\right)$$

d. h. mit Rücksicht auf die Integralformeln

$$\frac{1}{(g+k)^{\frac{n}{2}}} < \int_{g+k-1}^{g+k} \frac{dx}{x^{\frac{n}{2}}}$$

$$\int_g^\infty \frac{dx}{x^{\frac{n}{2}}} = \frac{1}{\left(\frac{n}{2}-1\right) g^{\frac{n}{2}-1}} = \gamma_{\frac{n}{2}-1}$$

zwischen den Grenzen $1 \pm \gamma_{\frac{n}{2}-1}$.

Zweitens liegt das Produkt

$$\Pi\left(1+\left(\frac{(-1)^{\frac{n}{2}}\Delta R^2}{p}\right)\frac{1}{p^{\frac{n-2}{2}}}\right)$$

zwischen den Grenzen

$$\Pi\left(1+\frac{1}{p^{\frac{n-2}{2}}}\right) < 1 + \frac{1}{(g+1)^{\frac{n-2}{2}}} + \frac{1}{(g+2)^{\frac{n-2}{2}}} + \cdots < 1 + \gamma_{\frac{n}{2}-2}$$

und $\Pi\left(1-\frac{1}{p^{\frac{n-2}{2}}}\right)$; da nun

$$\frac{1}{\Pi\left(1-\frac{1}{p^{\frac{n-2}{2}}}\right)} = \Pi\left(1+\frac{1}{p^{\frac{n-2}{2}}}+\frac{1}{p^{2\cdot\frac{n-2}{2}}}+\cdots\right)$$

jedenfalls kleiner ist als

$$1 + \frac{1}{(g+1)^{\frac{n-2}{2}}} + \frac{1}{(g+2)^{\frac{n-2}{2}}} + \cdots,$$

so ist

$$\Pi\left(1-\frac{1}{p^{\frac{n-2}{2}}}\right) > \frac{1}{1 + \frac{1}{(g+1)^{\frac{n-2}{2}}} + \frac{1}{(g+2)^{\frac{n-2}{2}}} + \cdots}$$

$$> 1 - \gamma_{\frac{n}{2}-2},$$

und somit liegt das betrachtete Produkt zwischen $1 \pm \gamma_{\frac{n}{2}-2}$.

Da ferner

$$(8\Delta R)_n \cdot S_n = \prod \frac{1}{1 - \frac{1}{p^n}}$$

gesetzt werden darf, wenn p alle nicht in $8\Delta R$ aufgehenden Primzahlen bedeutet, findet es sich aus derselben Betrachtung zwischen 1 und $1 + \gamma_{n-1}$ enthalten. Endlich hat man noch nach bekannter Formel*)

$$\lim_{\varrho=0} \varrho \sum \frac{1}{m^{1+\varrho}} = \frac{(8\Delta R)_1}{2^{2+\mathfrak{d}+\mathfrak{r}}},$$

denn die Zahlen m, auf welche sich die Summation bezieht, sind alle zu $8\Delta R$ prime positive Zahlen, welche die durch die $2 + \mathfrak{d} + \mathfrak{r}$ Symbole (52) vorgeschriebenen quadratischen Charaktere haben, d. h. sie sind die Individuen von

$$\frac{1}{2^{2+\mathfrak{d}+\mathfrak{r}}} \cdot \varphi(8\Delta R) = \frac{8\Delta R \cdot (8\Delta R)_1}{2^{2+\mathfrak{d}+\mathfrak{r}}}$$

arithmetischen Progressionen von der Form $8\Delta Rz + m_0$, für deren jede einzelne die Summe den Grenzwerth $\frac{1}{8\Delta R}$ hat.

Durch alles dies schliesst man aus der Gleichung (83) folgende zwei Ungleichheiten:

$$\frac{1}{1 + \gamma_{n-1}} \cdot \left(1 - \gamma_{\frac{n}{2}-1}\right) \cdot M_0 < 1 + \gamma_{\frac{n}{2}-2}$$

$$1 \cdot \left(1 + \gamma_{\frac{n}{2}-1}\right) \cdot M_0 > 1 - \gamma_{\frac{n}{2}-2}.$$

Da nun mit wachsendem g die Grössen γ sämmtlich gegen Null convergiren, so convergiren die Grenzen, zwischen denen M_0 enthalten bleibt, ersichtlich gegen Eins und somit kann auch M_0 nur gleich 1 sein. Auf solche Weise ist nun die Formel (51 a) vollkommen erwiesen. Durch ganz entsprechende Betrachtung aber schliesst man aus der für ein ungerades n in Frage kommenden Gleichung (85) denselben Werth 1 für M_0 und also auch die Allgemeingiltigkeit der Formel (51 b).

13. St. Smith hat in seiner Arbeit On the Orders and Genera of Quadratic Forms containing more than three Indeterminates (Proceedings of the R. Society 16 auf S. 203) für

*) Vgl. Analyt. Zahlenth. S. 83 Formel (21).

das Maass eines Geschlechts von Formen mit n Veränderlichen die nachstehenden Formeln aufgestellt:

Wenn n gerade ist, $n = 2\nu$:

$$M = \zeta_n \cdot \prod \chi(d) \cdot \mathsf{B}_n \cdot \sqrt{\Omega} \cdot \frac{1}{\pi^{\frac{n}{2}}} \sum \left(\frac{D}{h}\right) \frac{1}{h^{\frac{n}{2}}}, \tag{86}$$

wo

$$D = (-1)^{\frac{n}{2}} \cdot o_1 o_3 \cdots o_{n-1}$$

gesetzt ist und die Summe sich über alle positive zu $2D$ prime Zahlen bezieht; d ist jeder ungerade Primfaktor von Δ;

Wenn n ungerade ist, $n = 2\nu + 1$:

$$M = \zeta_n \cdot \prod \chi(d) \cdot \mathsf{B}_n \cdot \sqrt{\Omega}. \tag{87}$$

Gemäss der diesen Formeln hinzugefügten Erklärung der Zeichen überzeugt man sich unschwer, dass dieselben für den Fall ungerader Formen mit ungerader Determinante resp. mit den obigen Gleichungen (51a), (51b) völlig übereinkommen. Der Erklärung entsprechend ist nämlich zuerst

wenn n gerade ist,

$$\mathsf{B}_n = \frac{1}{2} B_1 \cdot \frac{1}{2} B_2 \cdots \frac{1}{2} B_{\frac{n-2}{2}},$$

wenn n ungerade ist,

$$\mathsf{B}_n = \frac{\frac{1}{2} B_1 \cdot \frac{1}{2} B_2 \cdots \frac{1}{2} B_{\frac{n-1}{2}}}{1 \cdot 2 \cdots \frac{n-1}{2}}.$$

Ferner ist für ein ungerades n

$$\chi(d) = E(d);$$

zur Uebereinstimmung der Formel (87) mit (51b) ist also erforderlich, dass $\zeta_n = 2E(2)$ d. i. nach nr. 9 des achten Capitels

$$\zeta_n = \frac{1}{\mathfrak{b}_1} = \frac{1}{2^{\frac{n-1}{2}}}\left(2^{\frac{n-1}{2}} + \delta\right) \tag{88}$$

ist.

Für ein gerades n wäre dagegen

$$\chi(d) = E(d)$$

zu setzen, falls d Primfaktor von D; ist aber d ein Primfaktor d' von $\varDelta$, der nicht in D aufgeht, so wäre

$$\chi(d) = E(d) \cdot \left(1 - \left(\frac{D}{d}\right) \frac{1}{d^{\frac{n}{2}}}\right).$$

Nun ist, da $(-1)^{\frac{n}{2}} \varDelta : D$ eine Quadratzahl,

$$\sum \left(\frac{D}{h}\right) \frac{1}{h^{\frac{n}{2}}} \cdot \prod \left(1 - \left(\frac{D}{d'}\right) \frac{1}{d'^{\frac{n}{2}}}\right) = \sum \left(\frac{(-1)^{\frac{n}{2}} \varDelta}{m}\right) \frac{1}{m^{\frac{n}{2}}},$$

wenn letztere Summation auf alle zu $2\varDelta$ prime positive Zahlen m bezogen wird; zur Uebereinstimmung der Formeln (86), (51a) ist mithin wieder erforderlich, dass

$$\zeta_n = 2E(2) = \frac{1}{\mathfrak{b}_1}$$

d. h. wenn $\varepsilon = +1$,

(89a) $$\zeta_n = \frac{1}{2^{\frac{n}{2}-1}} \left(2^{\frac{n}{2}-1} + \delta\right)$$

wenn $\varepsilon = -1$,

(89b) $$\zeta_n = 1.$$

Diese Werthe stimmen aber mit den von Stephen Smith angegebenen vollkommen überein. Es genüge, dies für die Formel (88) zu erweisen. Nach (52) des siebenten Capitels ist

$$\delta = (-1)^{\left[\frac{n}{4}\right] + \sigma + \psi(o, n-1)} \cdot \varepsilon^{\left[\frac{n}{2}\right]},$$

wo

$$\varepsilon = (-1)^{\left[\frac{n}{2}\right] + \nu},$$

ν gerade oder ungerade ist, jenachdem $\varDelta \equiv 1$ oder -1 (mod. 4), und

$$\sigma = \frac{1}{4}(d_1 - 1)(d_2 + 1) + \frac{1}{4}(d_2 - 1)(d_3 + 1) + \cdots$$
$$+ \frac{1}{4}(d_{n-2} - 1)(d_{n-1} + 1)$$

ist. Zunächst ist einfach zu erkennen, dass letztere Zahl mit der anderen

$$(90)\quad \sigma_0 = \frac{1}{4}(o_1 - 1)(o_2 + 1) + \frac{1}{4}(o_2 - 1)(o_1 o_3 + 1) + \frac{1}{4}(o_1 o_3 - 1)(o_2 o_4 + 1) + \cdots$$

(mod. 2) congruent ist. Setzt man folglich

$$\varepsilon_n = (-1)^{\sigma_0 + \psi(o, n-1)},$$

so wird, falls $n = 4\lambda + 1$ also

$$\left[\frac{n}{4}\right] = \lambda, \left[\frac{n}{2}\right] = 2\lambda$$

ist, $\delta = (-1)^\lambda \varepsilon_n$ also

$$\zeta_n = \frac{1}{2^{\frac{n-1}{2}}}\left(2^{\frac{n-1}{2}} + (-1)^\lambda \varepsilon_n\right);$$

falls aber $n = 4\lambda + 3$ also

$$\left[\frac{n}{4}\right] = \lambda, \left[\frac{n}{2}\right] = 2\lambda + 1$$

und $\varepsilon = (-1)^{\nu+1}$ also $+1$ oder -1 ist, jenachdem

$$\Delta \equiv -1 \text{ oder } +1 \pmod{4},$$

so ist je nach diesen beiden Fällen

$$\delta = (-1)^\lambda \varepsilon_n \text{ oder } \delta = (-1)^{\lambda+1} \varepsilon_n;$$

versteht man also mit Smith unter dem Zeichen D das Produkt

$$D = (-1)^{\left[\frac{n}{2}\right]} \cdot o_{n-1} o_{n-3} \cdots o_{n-2\left[\frac{n}{2}\right]+1},$$

sodass $\Delta = (-1)^{\left[\frac{n}{2}\right]} \cdot D \cdot Q^2$ gesetzt werden kann, so findet sich in beiden Fällen

$$\delta = (-1)^{\lambda + \frac{D-1}{2}} \cdot \varepsilon_n$$

also

$$\zeta_n = \frac{1}{2^{\frac{n-1}{2}}}\left(2^{\frac{n-1}{2}} + (-1)^{\lambda + \frac{D-1}{2}} \cdot \varepsilon_n\right).$$

Das sind aber die für ein ungerades n von Smith für ζ_n vorgeschriebenen Werthe, und ebenso bestätigen sich die für ein gerades n von ihm aufgestellten:

falls $n = 4\lambda$:

$$\zeta_n = \frac{1}{2^{\frac{n}{2}-1}}\left(2^{\frac{n}{2}-1} + (-1)^\lambda \varepsilon_n\right) \text{ oder } 1,$$

falls $n = 4\lambda + 2$:

$$\zeta_n = \frac{1}{2^{\frac{n}{2}-1}}\left(2^{\frac{n}{2}-1} + (-1)^\lambda \varepsilon_n\right) \text{ oder } 1,$$

je nachdem das dann geltende $D \equiv 1$ oder -1 (mod. 4). —

14. Um die bewiesenen Formeln anzuwenden, betrachte man zuerst dasjenige Geschlecht von Formen $b(y_\varrho)$ mit fünf Veränderlichen, welches, wenn b ungerade ist, die Ordnung

$$\begin{matrix} 1, & 1, & 1, & b \\ 1, & 1, & 1, & 1 \end{matrix}$$

hat und für alle β Primfaktoren q von b die Bedingung

$$\left(\frac{b_4}{q}\right) = \left(\frac{-1}{q}\right)$$

erfüllt. Die Formel (51 b) giebt dann für das Maass M desselben den Ausdruck

$$M = \frac{1}{2}\,\frac{B_1 B_2}{1 \cdot 2} \cdot \sqrt{\Omega} \cdot E(2) \prod E(q).$$

Nun ist

$$\Omega = b^4,\; B_1 = \frac{1}{6},\; B_2 = \frac{1}{30},$$

ferner findet sich

$$E(2) = \frac{1}{8}(4 + \delta)$$

$$E(q) = \frac{1}{2}\left(1 + \left(\frac{-1}{q}\right)\frac{1}{q^2}\right),$$

endlich ist

$$\delta = (-1)^{1+\sigma_0} \cdot (-1)^{\psi(o,4)},$$

wo σ_0 der Formel (90) gemäss zu bestimmen, hier also gleich Null, während

$$(-1)^{\psi(o,4)} = \prod_{m=1}^{4}\left(\frac{f_m'}{o_m}\right) = \left(\frac{b_4}{b}\right) = \left(\frac{-1}{b}\right)$$

ist, also wird

$$\delta = -\left(\frac{-1}{b}\right).$$

Demnach kommt

$$M = \frac{1}{2^5 \cdot 180}\left(4 - \left(\frac{-1}{b}\right)\right) \cdot \frac{b^2}{2^\beta} \cdot \prod\left(1 + \left(\frac{-1}{q}\right)\frac{1}{q^3}\right).$$

Da nun, wenn A die Anzahl der eigentlichen Darstellungen der Zahl b als Summe von sechs Quadraten bezeichnet, $\frac{A}{2^5 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}$ das Maass derselben ist, dies selbe Maass aber auch durch $2^\beta \cdot M$ ausgedrückt werden kann, findet sich für A der Ausdruck

$$A = 4\left(4 - \left(\frac{-1}{b}\right)\right) \cdot b^2 \cdot \prod\left(1 + \left(\frac{-1}{q}\right)\frac{1}{q^3}\right).$$

Hieraus aber erhält man durch ganz dieselben Betrachtungen wie bei der Darstellung durch vier Quadrate für die Anzahl sämmtlicher (eigentlichen und uneigentlichen) Darstellungen der Zahl b als Summe von sechs Quadraten den Werth

$$4\left(4 - \left(\frac{-1}{b}\right)\right) \cdot \prod_{q_1}\left(q_1^{2h_1} + q_1^{2h_1-2} + \cdots + 1\right)$$
$$\cdot \prod_{q_2}\left(q_2^{2h_2} - q_2^{2h_2-2} + \cdots \pm 1\right),$$

wenn man mit q_1, q_2 die Primfaktoren von b bezeichnet, die resp. von der Form $4x + 1$, $4x + 3$ sind und

$$b = q_1^{h_1} q_2^{h_2} \cdots$$

voraussetzt. Diese Formel liefert offenbar folgenden schon von Eisenstein gegebenen Satz: Die Anzahl *aller* Darstellungen einer ungeraden Zahl b als Summe von sechs Quadraten ist, wenn $b \equiv 1$ (mod. 4), gleich dem 12-fachen, wenn $b \equiv 3$ (mod. 4), gleich dem — 20-fachen Unterschiede zwischen der Summe der Quadrate derjenigen ihrer Faktoren, welche die Form $4x + 1$, und der Summe der Quadrate derjenigen, welche die Form $4x + 3$ haben*).

Betrachtet man ferner, indem man unter b eine ungerade Zahl versteht, welche aus β Primfaktoren zusammengesetzt ist, das Geschlecht derjenigen Formen $b(y_\varrho)$ der Ordnung

*) Eisenstein, Neue Theoreme der höheren Arithmetik (gegen Ende der Abhandlung) im J. f. d. r. u. a. Math. von Crelle 35.

$$1,\ 1,\ 1,\ 1,\ 1,\ b$$
$$1,\ 1,\ 1,\ 1,\ 1,\ 1$$

für welches

$$\left(\frac{b_6}{q}\right) = \left(\frac{-1}{q}\right)$$

ist, so findet man in gleicher Weise für sein Maass M den Ausdruck

$$M = \frac{1}{24 \cdot 180 \cdot 42} \cdot \frac{b^3}{2^\beta} \cdot \frac{8+\delta}{16} \cdot \prod \left(1 + \frac{1}{q^3}\right).$$

Da aber

$$\delta = (-1)^{1+\sigma_0} \cdot (-1)^{\psi(o,6)} \cdot \varepsilon \text{ und } \varepsilon = (-1)^{1+\nu},$$

ν aber gerade oder ungerade ist, je nachdem $b \equiv 1$ oder -1 (mod. 4) ist, findet sich wegen der Beziehung

$$(-1)^{\psi(o,6)} = \prod_1^6 \left(\frac{f_m'}{o_m}\right) = \left(\frac{-1}{b}\right)$$

je nach den unterschiedenen Fällen

$$\delta = \pm \left(\frac{-1}{b}\right)$$

d. h. stets gleich 1 und somit

$$M = \frac{1}{24 \cdot 180 \cdot 42} \cdot \frac{b^3}{2^\beta} \cdot \frac{9}{16} \cdot \prod \left(1 + \frac{1}{q^3}\right).$$

Daraus folgt, wenn A die Anzahl der eigentlichen Darstellungen von b als Summe von acht Quadraten, also $\frac{A}{2^7 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8}$ ihr Maass bezeichnet,

$$A = 16 \cdot b^3 \cdot \prod \left(1 + \frac{1}{q^3}\right),$$

und mit Hilfe dieses Ergebnisses wieder der allgemeinere Satz*): Die Anzahl *aller* Darstellungen einer ungeraden Zahl als Summe von acht Quadraten ist gleich der 16-fachen Summe der Kuben ihrer Faktoren.

Handelt es sich jetzt um die Darstellungen einer ungeraden Zahl b als Summe von sieben Quadraten, so ist analog wie im Falle von fünf Quadraten zu bemerken, dass es nur eine einzige Classe, also auch nur ein einziges Geschlecht von

---

*) S. ebendaselbst.

Formen der Ordnung

$$\begin{matrix} 1, & 1, & 1, & 1, & 1, & 1 \\ 1, & 1, & 1, & 1, & 1, & 1 \end{matrix}$$

giebt, als deren Repräsentant die Form

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2$$

angesehen werden kann. Zur Bestimmung der Anzahl aller eigentlichen Darstellungen von b durch diese Form bedarf es des Maasses der zwei mit $\Gamma_{(\mathrm{I})}$ und $\Gamma_{(\mathrm{II})}$ bezeichneten Geschlechter von Formen $b(y_\varrho)$ mit 6 Veränderlichen; das erste derselben von der Ordnung

$$\begin{matrix} 1, & 1, & 1, & 1, & b \\ 1, & 1, & 1, & 1, & 1 \end{matrix}$$

und den Charakteren

$$\left(\frac{b_5}{q}\right) = \left(\frac{-1}{q}\right)$$

ist stets vorhanden, das zweite jedoch, welches der Ordnung

$$\begin{matrix} 1, & 1, & 1, & 1, & b \\ 2, & 1, & 2, & 1, & 2 \end{matrix}$$

angehört, nur dann — was man durch ähnliche Betrachtungen zeigt wie in jenem Falle — wenn $b \equiv 7 \pmod{8}$ ist.

Nach der Formel (51a) ergiebt sich aber

$$M_{(\mathrm{I})} = \frac{1}{2} B_1 B_2 \cdot b^2 \sqrt{b} \cdot E(2) \cdot \prod E(q) \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}.$$

Hier wird, da

$$\varepsilon = (-1)^{\left[\frac{n}{2}\right] + \nu} = \pm 1$$

ist, je nachdem ν ungerade oder gerade d. i. $b \equiv 3$ oder $1 \pmod{4}$ angenommen wird, nach der Formel (59) des achten Capitels

für $b \equiv 1 \pmod{4}$

$$E(2) = \frac{1}{2}$$

für $b \equiv 3 \pmod{4}$

$$E(2) = \frac{1}{8}(4 + \delta),$$

während

$$E(q) = \frac{1}{2}$$

gefunden wird. Somit kommt

(91) $$M_{(I)} = \frac{1}{360} E(2) \cdot \frac{b^2\sqrt{b}}{2^\beta} \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}.$$

Dagegen wird

$$M_{(II)} = \frac{1}{2} B_1 B_2 \cdot \frac{b^2\sqrt{b}}{8} \cdot E(2) \prod E(q) \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3},$$

wo nun, weil nach der Formel (69) des achten Capitels

$$f[2] = 2^2\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{2^4}\right)\left(1-\frac{1}{2^6}\right)\cdot\left(1+\left(\frac{2}{b}\right)\frac{1}{8}\right)^{-1}$$

und $b \equiv 7 \pmod{8}$ ist,

$$E(2) = \frac{2^4}{63}\left(1+\left(\frac{2}{b}\right)\frac{1}{8}\right) = \frac{2}{7}$$

gefunden wird. Man erhält folglich

(92) $$M_{(II)} = \frac{1}{28 \cdot 360} \cdot \frac{b^2\sqrt{b}}{2^\beta} \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}.$$

Ist aber A die Anzahl der eigentlichen Darstellungen von b als Summe von sieben Quadraten, so ist,

wenn $b \equiv 1, 3, 5 \pmod{8}$

$$A = 2^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 2^\beta M_{(I)}$$

wenn $b \equiv 7 \pmod{8}$

$$A = 2^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 2^\beta (M_{(I)} + M_{(II)}).$$

Somit findet sich aus (91) und (92)

wenn $b \equiv 1, 5 \pmod{8}$

(93[1]) $$A = 448 \cdot b^2\sqrt{b} \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3},$$

wenn $b \equiv 3 \pmod{8}$, in welchem Falle, wie im folgenden

$$\delta = (-1)^{1+\psi(o,5)} = -\prod_1^5 \left(\frac{f'_m}{o_m}\right) = -\left(\frac{-1}{b}\right) = 1$$

ist,

(93[2]) $$A = 560 \cdot b^2\sqrt{b} \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3},$$

wenn endlich $b \equiv 7 \pmod{8}$, da

$$\frac{4+\delta}{8} + \frac{1}{28} = \frac{37}{56} \text{ ist,}$$

(93[3]) $$A = 592 \cdot b^2\sqrt{b} \cdot \frac{1}{\pi^3} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}.$$

In diesen Formeln erstreckt sich die Summation mit Bezug auf m über alle positive zu $2b$ prime Zahlen m. —

15. Die Formeln für das Maass eines Geschlechts weisen einen wesentlichen Unterschied darin auf, dass diejenigen für das Maass eines Geschlechts von Formen mit einer geraden Anzahl Veränderlichen die Summe

$$(94) \qquad \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}}$$

zum Faktor haben, der im Falle einer ungeraden Anzahl von Veränderlichen fehlt. Dieser Unterschied überträgt sich, wie man sieht, auch auf die Anzahl der Darstellungen einer Zahl b durch eine Summe von Quadraten. Diejenigen Formeln, welche die letztere Anzahl für 4, 6, 8 Quadrate ausdrücken, lassen einen innigen Zusammenhang derselben mit der Summe der Theiler von b resp. ihrer Quadrate oder Kuben erkennen. Ganz anders verhalten sich die Formeln für die Anzahl der Darstellungen von b als Summe von 3, 5, 7 Quadraten, aber unter einander zeigen diese wieder einen analogen Charakter, insofern die Ausdrücke für jene Anzahl resp. die Summe

$$(95) \qquad \sum \left(\frac{-b}{m}\right) \frac{1}{m}, \quad \sum \left(\frac{b}{m}\right) \frac{1}{m^2}, \quad \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}$$

als Faktor enthalten. Aehnlich wie Dirichlet es für die erste dieser drei Summen gethan hat und wir gelegentlich der Anzahl der Darstellungen einer Zahl durch die Summe dreier Quadrate entwickelt haben, lassen sich auch die beiden anderen, allgemeiner die Summe (94) summiren und es zeigt sich, dass ihre Werthe in entsprechender Weise von den ganzen Zahlen abhangen, welche unterhalb gewisser Grenzen liegen und gewisse entgegengesetzte quadratische Charaktere haben. Um sich von diesem Umstande zu überzeugen, kann man sich der Formeln bedienen, welche Cauchy in der 12. Note zu seinem grossen mémoire sur la théorie des nombres, in den mém. de l'Ac. des Sciences, Paris 1840, t. 17 gegeben hat.

I. Nennt man nämlich P eine aus lauter verschiedenen Primfaktoren bestehende ungerade positive Zahl und h, k alle zu P primen Zahlen $< P$, für welche resp.

$$\left(\frac{h}{P}\right) = +1, \quad \left(\frac{k}{P}\right) = -1 \tag{96}$$

ist, setzt

$$\varDelta_m = \sum_h h^m - \sum_k k^m$$

oder auch, indem man, wie üblich, das Legendre'sche Symbol $\left(\frac{s}{P}\right) = 0$ setzt, wenn s mit P einen gemeinsamen Theiler hat,

$$\varDelta_m = \sum_1^{P-1} \left(\frac{s}{P}\right) s^m, \tag{97}$$

endlich

$$J_m = \sum \left(\frac{s}{P}\right) \frac{1}{s^m}, \tag{98}$$

die Summe auf sämmtliche zu P prime positive Zahlen s ausgedehnt, so bestehen nach Cauchy folgende Gleichungen:

1) wenn $P \equiv 1$ (mod. 4), für gerade m

$$\left\{\begin{aligned} \varDelta_m &= 2P^{m+\frac{1}{2}}\left(\frac{m}{(2\pi)^2} J_2 - \frac{m(m-1)(m-2)}{(2\pi)^4} J_4 + \cdots \right. \\ &\qquad \left. \pm \frac{m(m-1)\cdots 3 \cdot 2}{(2\pi)^m} J_m\right) \\ &\text{für ungerade } m \\ \varDelta_m &= 2P^{m+\frac{1}{2}}\left(\frac{m}{(2\pi)^2} J_2 - \frac{m(m-1)(m-2)}{(2\pi)^4} J_4 + \cdots \right. \\ &\qquad \left. \pm \frac{m(m-1)\cdots 4 \cdot 3}{(2\pi)^{m-1}} J_{m-1}\right); \end{aligned}\right. \tag{99}$$

aus diesen beiden Formeln lassen sich dann die sämmtlichen Ausdrücke J_m mit geradem Index m berechnen und man findet insbesondere

wenn $P \equiv 1$ (mod. 4)

$$J_2 = \frac{\pi^2}{P^{5/2}} \cdot \varDelta_2. \tag{100}$$

2) wenn $P \equiv 3 \pmod{4}$, für gerade m

$$(101) \begin{cases} \Delta_m = -2P^{m+\frac{1}{2}}\left(\frac{1}{2\pi}J_1 - \frac{m(m-1)}{(2\pi)^3}J_3 + \cdots \right. \\ \qquad\qquad \left. \pm \frac{m(m-1)\cdots 4\cdot 3}{(2\pi)^{m-1}}J_{m-1}\right), \\ \text{für ungerade } m \\ \Delta_m = -2P^{m+\frac{1}{2}}\left(\frac{1}{2\pi}J_1 - \frac{m(m-1)}{(2\pi)^3}J_3 + \cdots \right. \\ \qquad\qquad \left. \pm \frac{m(m-1)\cdots 3\cdot 2}{(2\pi)^m}J_m\right); \end{cases}$$

aus diesen beiden Formeln lassen sich dann sämmtliche Ausdrücke J_m mit ungeradem Index m finden, z. B. ist,

wenn $P \equiv 3 \pmod{4}$

$$(102) \qquad J_1 = -\frac{\pi}{P^{3/2}}\Delta_1, \quad J_3 = \frac{2\pi^3}{3P^{7/2}}(\Delta_3 - P^2 \cdot \Delta_1).$$

II. Dieselben Formeln (99), (101) finden aber auch statt, wenn h, k alle zu $2P$ prime Zahlen $< 4P$ bezeichnen, für welche resp.

$$(103) \qquad (-1)^{\frac{h-1}{2}}\left(\frac{h}{P}\right) = +1, \quad (-1)^{\frac{k-1}{2}}\left(\frac{k}{P}\right) = -1$$

ist, und

$$(104) \qquad \Delta_m = \frac{1}{2^{2m+1}} \cdot \sum_1^{4P-1} (-1)^{\frac{s-1}{2}}\left(\frac{s}{P}\right)s^m$$

desgleichen

$$(105) \qquad J_m = \sum (-1)^{\frac{s-1}{2}}\left(\frac{s}{P}\right)\frac{1}{s^m}$$

— die Summe auf alle zu $2P$ prime positive Zahlen s ausgedehnt — gesetzt wird; doch gelten alsdann die Formeln (99) und folglich auch (100) für $P \equiv 3 \pmod{4}$, die Formeln (101) und folglich auch (102) für $P \equiv 1 \pmod{4}$.

Dies vorausgeschickt, setzen wir jetzt

$$(-1)^{\frac{n}{2}}\Delta = (-1)^{\frac{n}{2}}P \cdot S^2,$$

wo S^2 die grösste in Δ enthaltene Quadratzahl, P also eine Zahl ist, wie die Formeln von Cauchy sie voraussetzen. Jenachdem

$$(-1)^{\frac{n}{2}}P \equiv 1 \text{ oder } 3 \pmod{4}$$

ist, setzen wir weiter

$$\theta = +1 \text{ oder } \theta = -1;$$

dann ist stets

$$\left(\frac{(-1)^{\frac{n}{2}} P}{s}\right) = \theta^{\frac{s-1}{2}} \cdot \left(\frac{s}{P}\right), \tag{106}$$

wenn s positiv und prim gegen $2P$ ist. Ferner erhält man leicht die Beziehung

$$\begin{cases} \sum \left(\frac{(-1)^{\frac{n}{2}} \Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}} = \prod_q \left(1 - \left(\frac{(-1)^{\frac{n}{2}} P}{q}\right) \frac{1}{q^{\frac{n}{2}}}\right) \\ \qquad \cdot \sum \left(\frac{(-1)^{\frac{n}{2}} P}{s}\right) \frac{1}{s^{\frac{n}{2}}}, \end{cases} \tag{107}$$

wo links die Summation auf alle zu 2Δ, rechts auf alle zu $2P$ primen positiven Zahlen und die Multiplikation auf alle ungeraden Primzahlen ausgedehnt werden muss, welche in S aber nicht in P aufgehen; besteht Δ aus lauter verschiedenen Primfaktoren, so fällt dieser Faktor weg. Endlich ist wegen (106)

wenn $(-1)^{\frac{n}{2}} P \equiv 1 \pmod{4}$,

$$\sum \left(\frac{(-1)^{\frac{n}{2}} P}{s}\right) \frac{1}{s^{\frac{n}{2}}} = \sum \left(\frac{s}{P}\right) \frac{1}{s^{\frac{n}{2}}} \tag{108}$$

d. h., wie man leicht einsieht, gleich

$$\left(1 - \left(\frac{2}{P}\right) \frac{1}{2^{\frac{n}{2}}}\right) \cdot J_{\frac{n}{2}}, \tag{109}$$

wenn das Zeichen J_m in dem unter I bezeichneten Sinne, dagegen,

wenn $(-1)^{\frac{n}{2}} P \equiv 3 \pmod{4}$ ist,

$$\sum \left(\frac{(-1)^{\frac{n}{2}} P}{s}\right) \frac{1}{s^{\frac{n}{2}}} = \sum (-1)^{\frac{s-1}{2}} \left(\frac{s}{P}\right) \frac{1}{s^{\frac{n}{2}}} = J_{\frac{n}{2}}, \tag{110}$$

wenn das Zeichen J_m in dem unter II bezeichneten Sinne genommen wird.

Die Beziehung (107) gestattet folglich, vermittelst der Cauchy'schen Formeln die Summe

$$\sum \left(\frac{(-1)^{\frac{n}{2}} \varDelta}{m}\right) \frac{1}{m^{\frac{n}{2}}}$$

in allen Fällen zu finden. Denn, ist

erstens $(-1)^{\frac{n}{2}} P \equiv 1 \pmod{4}$, so ist entweder $P \equiv 1 \pmod{4}$ und $\frac{n}{2}$ gerade, dann berechnet sich, wenn J_m, $\varDelta_m$ im Sinne der Formeln (98), (97) genommen werden, $J_{\frac{n}{2}}$ nach den Formeln (99);

oder es ist $P \equiv 3 \pmod{4}$ und $\frac{n}{2}$ ungerade, dann findet sich $J_{\frac{n}{2}}$ aus den Formeln (101). Ist aber

zweitens $(-1)^{\frac{n}{2}} P \equiv 3 \pmod{4}$, so ist entweder $P \equiv 1 \pmod{4}$ und $\frac{n}{2}$ ungerade, dann berechnet sich — die Zeichen $\varDelta_m$, J_m im Sinne der Formeln (104), (105) genommen — $J_{\frac{n}{2}}$ aus den Formeln (101);

oder es ist $P \equiv 3 \pmod{4}$ und $\frac{n}{2}$ gerade, dann bestimmt sich $J_{\frac{n}{2}}$ aus den Formeln (99).

16. Handelt es sich z. B. um die auf alle positive zu $2b$ prime Zahlen m bezogene Summe

$$\sum \left(\frac{b}{m}\right) \frac{1}{m^2},$$

und betrachten wir der Einfachheit wegen nur den Fall, wo b aus lauter verschiedenen Primfaktoren besteht, so ist P mit b zu identificiren.

Ist dann zuerst $b \equiv 1 \pmod{4}$, so kommt nach (109)

$$\sum \left(\frac{b}{m}\right) \frac{1}{m^2} = \left(1 - \left(\frac{2}{b}\right) \frac{1}{4}\right) \cdot J_2,$$

wo J_2 durch die Formel (100), $\varDelta_2$ aber durch (97) zu bestimmen d. h.

$$J_2 = \frac{\pi^2}{b^{5/2}} \cdot \sum_1^{b-1} \left(\frac{s}{b}\right) s^2$$

zu setzen ist; man findet also dann

$$\text{(111a)} \qquad \sum \left(\frac{b}{m}\right) \frac{1}{m^2} = \frac{\pi^2}{b^{5/2}} \left(1 - \left(\frac{2}{b}\right) \frac{1}{4}\right) \cdot \sum_1^{b-1} \left(\frac{s}{b}\right) s^2.$$

Ist dagegen zweitens $b \equiv 3 \pmod{4}$, so folgt aus (110)

$$\sum \left(\frac{b}{m}\right) \frac{1}{m^2} = J_2,$$

wo nun J_2 wieder durch die Formel (100), in dieser aber Δ_2 durch (104) zu bestimmen ist, man findet also dann

$$\text{(111b)} \qquad \sum \left(\frac{b}{m}\right) \frac{1}{m^2} = \frac{\pi^2}{2^5 \cdot b^{5/2}} \cdot \sum_1^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^2.$$

Handelt es sich andererseits um die Summe

$$\sum \left(\frac{-b}{m}\right) \frac{1}{m^3},$$

so ist, wenn zuerst $b \equiv 3 \pmod{4}$, nach (109)

$$\sum \left(\frac{-b}{m}\right) \frac{1}{m^3} = \left(1 - \left(\frac{2}{b}\right) \frac{1}{8}\right) \cdot J_3,$$

wo J_3 durch die Formel (102), in dieser aber Δ_1, Δ_3 durch (97) zu bestimmen sind; man findet demnach

$$\text{(112a)} \qquad \left\{ \begin{aligned} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3} &= \left(1 - \left(\frac{2}{b}\right) \frac{1}{8}\right) \cdot \frac{2\pi^3}{3 b^{7/2}} \\ &\cdot \left(\sum_1^{b-1} \left(\frac{s}{b}\right) s^3 - b^2 \cdot \sum_1^{b-1} \left(\frac{s}{b}\right) s\right). \end{aligned} \right.$$

Ist dagegen zweitens $b \equiv 1 \pmod{4}$, so folgt aus (110)

$$\sum \left(\frac{-b}{m}\right) \frac{1}{m^3} = J_3,$$

wo für J_3 die Formel (102) und in dieser für Δ_1, Δ_3 die Formel (104) anzuwenden ist, mithin wird

$$\text{(112b)} \qquad \left\{ \begin{aligned} \sum \left(\frac{-b}{m}\right) \frac{1}{m^3} &= \frac{\pi^3}{2^6 \cdot 3 b^{7/2}} \\ \cdot \left(\sum_1^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^3 \right. &- \left. 16 b^2 \cdot \sum_1^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s\right). \end{aligned} \right.$$

Von diesen Resultaten machen wir zunächst Gebrauch, um die Anzahl der sämmtlichen Darstellungen der Zahl b als Summe von fünf Quadraten unter endlicher Form zu erhalten.

1) Sei zuerst $b \equiv 1 \pmod{8}$. Die Formel (45b):

$$A_1 = \frac{80 \cdot b^{3/2}}{\pi^2} \cdot \sum \left(\frac{b}{m}\right) \frac{1}{m^2}$$

geht, wenn der Werth (111a), welcher der Summe jetzt zukommt, eingesetzt und die Gleichung $\left(\frac{2}{b}\right) = 1$ beachtet wird, in die folgende über:

$$A_1 = 60 \cdot \frac{1}{b} \sum_1^{b-1} \left(\frac{s}{b}\right) s^2. \tag{113}$$

Doch gelangt man zu einem einfacheren Ausdrucke, wenn man bedenkt, dass

$$\sum_1^{b-1} \left(\frac{s}{b}\right) s^2 = \sum_h h^2 - \sum_k k^2$$

ist. Wenn man nämlich mit h', k' diejenigen Zahlen h, k bezeichnet, die $< \frac{b}{2}$ sind, und mit α, γ ihre Anzahl, so kann

$$3 \cdot \sum h^2 = -\sum h^2 + \sum (2h)^2$$

in die Form

$$3 \cdot \sum h^2 = -\sum h^2 + \sum (2h')^2 + \sum (b - 2h')^2 \\ + 3\alpha b^2 - 4b \sum h'$$

gesetzt werden, die vermöge der Bemerkung, dass wegen $\left(\frac{2}{b}\right) = 1$

$$\sum (2h')^2 + \sum (b - 2h')^2 = \sum h^2$$

ist, vereinfacht

$$3 \cdot \sum h^2 = 3\alpha b^2 - 4b \sum h'$$

giebt; ebenso kommt

$$3 \cdot \sum k^2 = 3\gamma b^2 - 4b \sum k'.$$

Nun ist die Anzahl der h gleich derjenigen der k und wegen

$\left(\frac{b-s}{b}\right) = \left(\frac{s}{b}\right)$ auch die der h' gleich derjenigen der k' d. h. $\alpha = \gamma$. Man findet mithin sogleich

$$3 \cdot \left(\sum h^2 - \sum k^2\right) = 4b\left(\sum k' - \sum h'\right)$$

und daraus

$$A_1 = -80 \cdot \sum \left(\frac{s}{b}\right) s, \quad \left(s < \frac{b}{2}\right). \tag{114}$$

2) Ist zweitens $b \equiv 5 \pmod{8}$, so findet man, da jetzt $\left(\frac{2}{b}\right) = -1$ ist, ganz entsprechend auf Grund der Formel (45c)

$$A_5 = 140 \cdot \frac{1}{b} \sum_1^{b-1} \left(\frac{s}{b}\right) s^2, \tag{115}$$

und für dieselbe Anzahl mittels gleicher Betrachtungen wie zuvor den andern Ausdruck

$$A_5 = -112 \cdot \sum \left(\frac{s}{b}\right) s, \quad \left(s < \frac{b}{2}\right). \tag{116}$$

Ist 3) $b \equiv 3, 7 \pmod{8}$ also $\left(\frac{b-s}{b}\right) = -\left(\frac{s}{b}\right)$, so folgt auf Grund der Formeln (45a) und (111b)

$$A_{3,7} = \frac{5}{b} \sum_1^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^2. \tag{117}$$

Diese Summe nimmt zunächst, wenn man sie in zwei zerlegt, welche von 1 bis $2b$ und von $2b$ bis $4b$ reichen, und in der ersten s durch $2b - s$, in der zweiten s durch $2b + s$ ersetzt, die Gestalt an:

$$-\sum_1^{2b} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) (2b - s)^2 - \sum_1^{2b} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) (2b + s)^2$$

oder, da $\sum_1^{2b} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) = 0$ ist, diese andere:

$$-2\sum_1^{2b} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^2.$$

Wird aber letztere Summe wieder in zwei andere zerlegt, welche von 1 bis b und von b bis $2b$ reichen, und man setzt

in der ersteren $s = b - 2t$, in der zweiten $s = b + 2t$, sodass dann t von 1 bis $\left[\frac{b}{2}\right]$ reicht, so verwandelt sich der Ausdruck in folgenden

$$\begin{aligned} &-2 \cdot \left(\frac{2}{b}\right) \cdot \sum (-1)^t \left(\frac{t}{b}\right)(b-2t)^2 \\ &+2 \cdot \left(\frac{2}{b}\right) \cdot \sum (-1)^t \left(\frac{t}{b}\right)(b+2t)^2 \\ &= 16b \cdot \left(\frac{2}{b}\right) \sum (-1)^t \left(\frac{t}{b}\right) t. \end{aligned}$$

Demnach erhält man neben (117) noch folgende Formeln, indem man die Fälle $b \equiv 3$, $b \equiv 7$ (mod. 8) trennt:

$$(118) \qquad \left\{ \begin{aligned} A_3 &= -80 \cdot \sum (-1)^t \left(\frac{t}{b}\right) t \\ A_7 &= +80 \cdot \sum (-1)^t \left(\frac{t}{b}\right) t \end{aligned} \right\} \left(t < \frac{b}{2}\right).$$

Diese und noch andere Ausdrücke für die Anzahl der Darstellungen einer Zahl als Summe von fünf Quadraten sind bereits von Eisenstein*) gegeben worden. Vgl. dazu Smith sur la représ. des nombres par une somme de cinq carrés, sowie auch seine oben angeführte Abh. in den Proceedings 1867 S. 207, wo noch allgemeinere Fälle berücksichtigt sind.

17. An derselben Stelle hat Eisenstein auch für die Anzahl der Darstellungen einer Zahl als Summe von sieben Quadraten analoge endliche Formeln mitgetheilt, die sich mittels unserer obigen Resultate bestätigen lassen. (S. auch Smith an der letzt-angeführten Stelle.)

1) Nach (93^3) ist, wenn zuerst $b \equiv 7$ (mod. 8) ist,

$$A_7 = \frac{592\, b^{5/2}}{\pi^3} \cdot \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}.$$

---

*) Eisenstein, note sur la représentation d'un nombre par la somme de 5 carrés, im Journ. f. d. r. u. a. Math. 35 S. 368. — Die Formeln (113) und (115) lassen den beachtenswerthen Umstand erkennen, dass, wenn $b \equiv 1$ (mod. 4) ist,

$$\sum h^2 > \sum k^2$$

sein muss. Für den Fall einer Primzahl b findet sich dieser Satz bereits ausgesprochen von Dirichlet, J. f. d. r. u. a. Math. 18 S. 270. Aehnliche Sätze folgen aus den Formeln der nächsten nr.

Bildet man die Summe nach (112a) und berücksichtigt, dass $\left(\frac{2}{b}\right) = 1$ ist, so kommt

$$(119) \qquad A_7 = \frac{37 \cdot 28}{3b}\left(\sum_1^{b-1}\left(\frac{s}{b}\right)s^3 - b^2\sum_1^{b-1}\left(\frac{s}{b}\right)s\right).$$

Wenn nun h', k' diejenigen Zahlen h, k sind, welche $< \frac{b}{2}$ sind, und α, γ ihre Anzahl, so kann man setzen

$$7 \cdot \sum h^3 = -\sum h^3 + \sum (2h)^3$$
$$= -\sum h^3 + \sum (2h')^3 + \sum (2b - 2k')^3$$

d. i. gleich

$$-\sum h^3 + \sum (2h')^3 + \sum (b - 2k')^3$$
$$+ 3b\sum (b - 2k')^2 + 3b^2\sum (b - 2k') + \gamma b^3,$$

oder, weil die $2h'$ die geraden, die $b - 2k'$ die ungeraden Zahlen h, zusammen also die $2h'$ und $b - 2k'$ die sämmtlichen h ausmachen, einfacher

$$7\sum h^3 = 7\gamma b^3 - 18b^2\sum k' + 12b\sum k'^2.$$

Ebenso kommt

$$7\sum k^3 = 7\alpha b^3 - 18b^2\sum h' + 12b\sum h'^2$$

also

$$7\sum\left(\frac{s}{b}\right)s^3 = 7(\gamma - \alpha)b^3 + 18b^2\left(\sum h' - \sum k'\right)$$
$$- 12\left(\sum h'^2 - \sum k'^2\right).$$

Andererseits kommt ebensowohl

$$\sum h = \sum h' + \sum (b - k') = \gamma b + \sum h' - \sum k'$$

als auch

$$\sum h = \sum 2h' + \sum (b - 2k') = \gamma b + 2\left(\sum h' - \sum k'\right)$$

mithin

$$\sum h' - \sum k' = 0$$

und

$$\sum h = \gamma b, \quad \sum k = \alpha b$$

$$7b^2 \cdot \sum\left(\frac{s}{b}\right)s = 7b^3(\gamma - \alpha).$$

Auf Grund dieser Ergebnisse findet man

$$A_7 = -\frac{37 \cdot 28}{3b} \cdot \frac{12}{7}\left(\sum h'^2 - \sum k'^2\right)$$

oder einfacher

(120) $$A_7 = -16 \cdot 37 \sum \left(\frac{s}{b}\right) s^2, \quad \left(s < \frac{b}{2}\right).$$

2) Wenn zweitens $b \equiv 3 \pmod{8}$ also $\left(\frac{2}{b}\right) = -1$, so erhält man zunächst nach (93[2]) und (112a)

(121) $$A_3 = \frac{420}{b}\left(\sum_1^{b-1}\left(\frac{s}{b}\right) s^3 - b^2 \sum_1^{b-1}\left(\frac{s}{b}\right) s\right).$$

Setzt man hier

$$9\sum h^3 = \sum h^3 + \sum (2h)^3,$$

so folgt nach einer analogen Umformung

$$9\sum h^3 = \sum h^3 + \sum k^3 + 7\gamma b^3 - 18 b^2 \sum k' + 12 b \sum k'^2$$

ebenso

$$9\sum k^3 = \sum k^3 + \sum h^3 + 7\alpha b^3 - 18 b^2 \sum h' + 12 b \sum h'^2$$

also

$$9\left(\sum h^3 - \sum k^3\right) = 7(\gamma - \alpha) b^3 + 18 b^2 \left(\sum h' - \sum k'\right)$$
$$- 12 b \left(\sum h'^2 - \sum k'^2\right).$$

Andererseits ist

$$\sum h = \sum h' + \sum (b - k') = \gamma b + \sum h' - \sum k'$$
$$\sum k = \alpha b + \sum k' - \sum h'$$

also

$$9\left(\sum h - \sum k\right) b^2 = 9(\gamma - \alpha) b^3 + 18 b^2 \left(\sum h' - \sum k'\right).$$

Mithin ergiebt sich nach (121)

$$A_3 = \frac{420}{9b}\left(2(\alpha - \gamma) b^3 - 12 b \sum \left(\frac{s}{b}\right) s^2\right)$$

oder einfacher

(122) $$A_3 = 8 \cdot 35 \left(\frac{b^2}{3}\sum\left(\frac{s}{b}\right) - 2\sum\left(\frac{s}{b}\right) s^2\right), \quad \left(s < \frac{b}{2}\right).$$

3) Sei endlich $b \equiv 1 \pmod{4}$, so ist nach (93[1])

$$A = \frac{448\, b^{5/2}}{\pi^3} \cdot \sum \left(\frac{-b}{m}\right) \frac{1}{m^3}$$

d. h. nach (112b)

$$A = \frac{7}{3b}\left(\sum_{1}^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^3 - 16b^2 \cdot \sum_{1}^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s\right).$$

Die Summe

$$\sum_{1}^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^3$$

kann aber zunächst durch Zerlegung folgendermassen geschrieben werden:

$$\sum_{1}^{2b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) [2b - s)^3 - (2b + s)^3]$$

$$= -2\sum_{1}^{2b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s^3 - 24b^2 \cdot \sum_{1}^{2b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s.$$

Ebenso kommt

$$\sum_{1}^{4b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s = -2\sum_{1}^{2b-1} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s.$$

Zerlegt man ferner das Intervall von 1 bis $2b - 1$ in seine beiden Hälften, so erhält man mittels einfacher Umformungen endlich

$$A = 28 \cdot \sum_{1}^{b} (-1)^{\frac{s-1}{2}} \left(\frac{s}{b}\right) s(2b - s).$$

Setzt man aber in dieser, den beiden Fällen $b \equiv 1$, $b \equiv 5$ (mod. 8) gemeinsamen Formel $s = b - 2t$, so geht sie in die Gestalt

$$A_{1,5} = 28 \cdot \left(\frac{2}{b}\right) \cdot \sum (-1)^t \cdot \left(\frac{t}{b}\right)(b^2 - 4t^2), \quad \left(t < \frac{b}{2}\right)$$

über und man findet somit

wenn $b \equiv 1$ (mod. 8),

$$\left.\begin{aligned} &(123) \qquad A_1 = 28 \cdot \sum (-1)^t \cdot \left(\frac{t}{b}\right)(b^2 - 4t^2) \\ &\qquad \text{wenn aber } b \equiv 5 \text{ (mod. 8) ist,} \\ &(124) \qquad A_5 = -28 \cdot \sum (-1)^t \cdot \left(\frac{t}{b}\right)(b^2 - 4t^2) \end{aligned}\right\} \left(t < \frac{b}{2}\right).$$

Die gefundenen Formeln stimmen mit den Eisenstein'schen überein. —

Der Erfolg der Methode, welche zur Aufsuchung der Anzahl aller Darstellungen einer Zahl als Summe von Quadraten angewandt worden ist, beruht wesentlich auf dem Umstande, dass, so lange $n \overline{\overline{<}} 8$, nur eine einzige Classe folglich auch nur ein einziges Geschlecht der Ordnung, zu welcher die Quadratsumme gehört, vorhanden ist. Für eine grössere Anzahl von Unbestimmten hört dieser Umstand auf (siehe darüber den dritten Abschnitt), und es würde daher weiterer Mittel bedürfen, jene Anzahl zu ermitteln. Ausser einem speciellen Satze über die Anzahl der Darstellungen einer Zahl als Summe von zehn Quadraten, welchen Eisenstein (an der citirten Stelle) noch anführt, haben sonst die in dieser Richtung angestellten Untersuchungen bisher kein weiteres Ergebniss aufzuweisen*). Sonach können wir unsere Darstellung derselben hiermit beschliessen. —

*) Allerdings hat Liouville in seinem Journale sér. 2 t. 5 p. 143 sowie t. 9 p. 296 über die Anzahl Darstellungen einer Zahl als Summe von 12, und t. 11 über die Anzahl der Darstellungen einer Zahl als Summe von 11 Quadraten Sätze mitgetheilt, doch ist bisher von ihnen kein rechter Beweis gegeben.

Berichtigungen.

Seite 37 Zeile 2 und 3 v. u. lies ps'' statt $p''s$ und ps' statt $p's$.
„ 125 letzte Zeile lies M'' statt M'.
„ 155 Zeile 11 lies wenigstens $m - 2$ statt $m - 2$.
„ 160 letzte Zeile desgleichen.
„ 186 Zeile 10 lies Ω statt ω.
„ 205 „ 8 v. u. lies Form statt Formel.
„ 218 „ 3 lies z statt z'.
„ 227 „ 16 lies aM statt M.
„ 228 „ 13 lies keine A, B entsprechenden ganzzahligen Auflösungen.
„ 258 Zeile 15 v. u. lies 1, 3, 5 statt 1, 5.
„ 259 „ 17 lies 1, 3, 5 statt 1 oder 5.
„ 293 ist zwischen Zeile 11 und 12 eine Reihe von Punkten zu denken.
„ 354 letzte Zeile lies 193 statt 192.
„ 370 Zeile 12 lies $\delta = 0$ statt $d = 0$.
„ 378 ist die Voraussetzung unerwähnt geblieben, dass die Determinanten von F_{a_0}, F_{b_0} nicht Null sind.
„ 445 Zeile 12 v. u. lies $1, 2, \ldots \lambda$ statt $12 \ldots \lambda$.
„ 475 „ 3 lies $p^{t-\nu_n-2}$ statt $p^{t-\nu_n-1-\nu_n-2}$.
„ 493 „ 5 lies $(-1)^{\frac{m}{2}}$ statt $(-1)^m$.
„ 550 Formel (68) ist die rechte Seite zu verdoppeln.
„ 551 „ (69) ist der erste Faktor $2^{\frac{n}{2}-1}$, nicht $2^{\frac{n}{2}}$.
„ 588 Zeile 6 lies zu statt zn.
„ 590 „ 9 v. u. lies $\mathfrak{f}_x(x_\varrho)$ statt $f_x(x_\varrho)$.
„ 616 „ 2 lies qua- statt qna-.
„ 618 „ 6 lies $\frac{1}{m^{2+2\varrho}}$ statt $\frac{2}{m^{2+2\varrho}}$.

„ 640 Absatz 3) ist zu berichtigen, wie folgt. Jeder Repräsentant des Geschlechts G, durch den m darstellbar ist, kann durch einen äquivalenten Hauptrepräsentanten f mit dem ersten Coefficienten $a_{11} = m$ ersetzt werden; für diesen besteht die Congruenz (81), wo α dieselbe Zahl bedeutet, wie bisher m. — Alles weitere bleibt ungeändert.



Im gleichen Verlag erschien von demselben Verfasser:

Bachmann, Paul, Zahlentheorie. Versuch einer Gesammtdarstellung dieser Wissenschaft in ihren Hauptheilen. In 6 Theilen. I. Theil: die Elemente der Zahlentheorie. [XII u. 264 S.] gr. 8. 1892. geh. n. ℳ 6.40.

Es kann wohl nur ein willkommenes Unternehmen genannt werden, eine Gesamtdarstellung des heutigen Standes der Zahlentheorie zu versuchen. Der Verfasser beabsichtigt nicht, ein Kompendium der Zahlentheorie zu schreiben, vielmehr, in einer Reihe von Einzeldarstellungen Bilder der einzelnen Hauptgebiete derselben zu entwerfen, welche von den hauptsächlichsten Forschungen, durch welche sie gewonnen worden sind, Kenntnis zu geben bestimmt sind.

Das gegenwärtige Werk hat die Elemente der Zahlentheorie zu seinem Gegenstande. Unter diesem Namen darf man jetzt füglich wohl alles das zusammenfassen, was Gaufs in den ersten fünf Abschnitten seiner Disquisitiones arithmeticae behandelt hat, soweit es nicht das Gebiet der binären quadratischen Formen überschreitet. Von der Darstellung bleibt alles, was mit der Verteilung der Formen in Geschlechter zusammenhängt, ausgeschlossen, weil der Hauptsatz dieser Theorie sich nicht aus jenem elementaren Gebiete ableiten läfst.

Näheres siehe Teubners Mitteilungen 1892 Nr. 3, S. 74.

——— ——— II. Theil: die analytische Zahlentheorie. [XVIII u. 494 S.] gr. 8. 1894 geh. n. ℳ 12.—

In diesem Werke sucht der Verfasser von denjenigen zahlentheoretischen Forschungen, welche auf analytische Methoden begründet sind, ein übersichtliches Bild zu entwerfen.

Das Werk beschränkt sich auf Fragen der reellen Zahlentheorie, welche die hauptsächlichsten zahlentheoretischen Funktionen oder die Theorie der binären quadratischen Formen betreffen, und schliefst alle Anwendungen der Theorie der elliptischen Funktionen auf Zahlentheorie, denen ein späteres Werk gewidmet werden soll, vollständig aus.

Näheres siehe Teubners Mitteilungen 1894 Nr. 1, S. 5.

——— ——— III. Theil: die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie. Akademische Vorlesungen. Mit Holzschnitten im Text und 1 lithogr. Tafel. [XII u. 300 S.] gr. 8. 1872. geh. n. ℳ 7.—

Voranzeige siehe Teubners Mitteilungen 1872 Nr. 1, S. 11.

——— Vorlesungen über die Natur der Irrationalzahlen. [X u. 151 S.] gr. 8. 1892. geh. n. ℳ 4.—

Nachdem in dem vorliegenden Werke die Irrationalzahlen, im wesentlichen im Anschlufs an Heines Gesichtspunkte, begrifflich festgestellt sind, wobei eine gröfsere Anschaulichkeit erreicht sein dürfte durch Einführung des Begriffes „zweier gegen einander konvergierender Wertreihen“, werden von den algebraischen Zahlen einige Fundamentalsätze hergeleitet, welche auf ihre allgemeinste Definition sich beziehen. Nach dem Grade der Gleichung, durch welche sie bestimmt werden, unterscheiden sie sich in quadratische, kubische Irrationellen u. s. f., und es fragt sich, welche rein arithmetischen Kennzeichen dieser algebraischen Einteilung adäquat sind. Hier wird nun zunächst das arithmetische Kennzeichen der quadratischen Irrationellen nach Lagrangeschen Gesichtspunkten hergeleitet, nachdem zuvor die elementare Grundlage der Herleitung, die Theorie der Kettenbrüche, mittels eines Algorithmus entwickelt worden, von welchem der Jacobische Kettenbruchalgorithmus nur eine einfache Verallgemeinerung ist. Dann folgt Liouvilles Nachweis von dem Vorhandensein nicht algebraischer Irrationellen und eine kurze Übersicht der Arbeiten, durch welche Lambert, Legendre und Liouville über die Natur der Zahlen e und π Licht zu verbreiten versucht haben. Ausführlich werden dann die Hermiteschen Arbeiten über die Zahl e in ihrem Zusammenhange dargestellt, und darauf ein Teil der Lindemannschen Untersuchung über die Ludolphsche Zahl gegeben, soweit es erforderlich ist, um von ihr eine genügende Vorstellung zu bilden; statt sie im ganzen zu entwickeln, zieht Verf. es vor, den Nachweis für die Transscendenz der Zahl π auf dem einfacheren Wege zu erbringen, welchen Weierstrafs uns gelehrt hat. Eine letzte Vorlesung giebt Kenntnis von den Kettenbruchalgorithmen von Jacobi und von den wenigen, noch unzureichenden Resultaten, zu denen der Versuch, ein Kennzeichen, ähnlich dem für die quadratischen Irrationellen gefundenen, auch für die kubischen zu ermitteln, bisher geführt hat.

Näheres siehe Teubners Mitteilungen 1892 Nr. 2, S. 46.



